Question 1:
- What system should be put in place to require the removal of harmful content from online platforms? For example, the direct involvement of the regulator in a notice and take down system where it would have a role in deciding whether individual pieces of content should or should not be removed on receipt of an appeal from a user who is dissatisfied with the response they have received to a complaint submitted to the service provider. [Sections 2, 4, & 8 of the explanatory note]

The proposed regulator is an important and evolutionary step forward that would provide important focus and coordination of the how Ireland manages illegal and harmful use of the Internet. Starting in 1998 with the first report on the Illegal and Harmful Use of the Internet, Ireland has been very progressive in positive initiatives to promote online safety among minors and adults alike and to combat illegal content and activity on the Internet. However, internet services are having a greater effect on everyday life of Irish citizens and there is a need for great focus on the impact on social networking services, the future of artificial intelligence, the growth in the internet-of-things, the planned growth in global satellite internet services and the increasing adoption of autonomous vehicles in the air and on the ground. A regulator focused on the dark side of the internet and providing trusted auditing of internet services will provide a necessary increase in trust for parents and children alike. The proposed regulator need a broad understanding of the complex issues facing the internet and needs to balance the rights of children and persons to free speech while simultaneously ensuring greater safety and trust for all. There are particular challenges that Ireland needs to aggressively address including online bullying and harmful behaviours leading to extremely serious harm. In addition, it is not clear which new services will be successful or what risks they include for internet users. There is an important role for the proposed regulator to ensure that the Internet service providers adhere to the highest standards of online behaviours and transparency and works with other countries to coordinate efforts to improve online services for all.

A) There are several important issues to be addressed in order to implement an effective Notice and Take Down system (NTD) regime. 1. Identifying suspicious content that needs action. Often the suspect internet content needs to be re-actively identified by members of the public who detect material during their regular internet use and then reported to the service provider and then the regulator. It is important that the range of content that can be addressed by the regulator is clearly elucidated and enumerated. In my opinion, the regulator should commence with a narrow remit that can be expanded as skills evolve and experience is gained. There might be situations where content can be proactively identified through pro-active internet searches but the volume of suspect content can be high, might not relate to the Irish or European market. In all cases content might be behind a pay-wall or accessible in a password protected area. 2. Technical specification of suspicious content that requires action. Suspect content can be
presented in different media technologies including audio, video, text or graphics and can be published using a complex variety of technical formats and can be further hidden using obfuscating technologies. Some of the primary platforms such as Google, YouTube, Facebook et al. offer internal reporting systems which automatically identify the specific details of the suspect material for review by trained moderators. Often members of the public can face difficulties in determining and recording the exact location of the suspicious content OR the content is dynamically presented in a manner that changes location regularly. An easy system of identifying content might require direct engagement/ cooperation / regulation of/with the content providers. 3. Which criteria and legal ‘rules’ to follow (Irish, EU, US, etc or Common Decency style rules, Company Terms and Conditions (T&C’s)?) Once suspicious content has been reported and referred for assessment, the receiving authority needs to have direct access to trained and skilled personnel to access the reported content and grade the content along agreed, transparent and clear criteria whilst respecting the views of the reporting person(s) and the intentions and target audience of the content author / publisher. This needs clear respect for human rights law and deep understanding of Irish, European and International law and understanding the impact of harmful content on vulnerable internet users. The reviewers can also be strongly impacted by constant viewing of wide-ranging harmful and deliberately provocative content and would need a positive supportive environment for long term effectiveness and personal mental health. Once the reported content has been assessed as harmful or in conflict with a provider’s T&C’s (or possibly illegal) the location of the content would need to be determined in order to decide which internet provider is most likely responsibility for taking action. Sometimes this might be obvious from the received report but sometimes this can be more complicated than first anticipated when content. 4. Liability in the decision making. A key concern by all parties is the issues of (a) false-positives (when content is identified as harmful / illegal when in fact it is not) and (b) false-negatives (when suspect content is identified as non-harmful/non-illegal when in fact it is) and who might be impacted by such failures and whether their might be legal recourse to such decisions. It could include charges of slander in the case of (a) and reduction in trust and confidence in the regulator in the case of (b). Since suspect content that is to be considered by the proposed regulator is intended to focus mainly on alleged harmful content, it is more difficult to make consistent reliable assessment of such content based on the emotional or psychological impact of such content on a complex selection of audiences. It would be very important that decisions reached by the regulator are clear and considered authoritative and protected against unreasonable and (for minor reasons) legal action. 5. Possible actions include content removal, content warning, disable publishing, prevent re-distribution, age-restriction controls, etc) Once suspect content is identified and located and once a decision has been made that the identified content is likely to be harmful it is then necessary to decide what actions can be taken in relation to such content. Actions might include asking the author to edit the content in order to stop the harm (noting that it can sometimes be technically and legally difficult to identify the authors), to ask the publisher to take down the content, to ask intermediaries to block content (noting that blocking internet content mechanisms are often quite trivial to circumvent), to request legal investigation or instigate legal investigation as to the purpose and motivations for the suspect content to be published in the first place or to request age-verification or geo-blocking “walled gardens” to be put in place to restrict access to content to
selected ages (assuming an age verification system (AVS) has been successfully designed and implemented. It is also important to determine whether such actions will be/should be restricted to certain geographical regions or to specific groups in society – such as age restrictions or special needs persons. Ensuring long term implementation of the decision is also challenging since content might be re-published or re-distributed on different platforms in different media formats with minor or significant changes affecting ease of technical identification. B) Adopting and adapting a model of regulated self-regulation or co-regulation where industry organisations work closely with the regulator. There is a significant role in close oversight by the regulator of the activities of the various internet service providers especially in identifying unforeseen emerging illegal and harmful activities. The regulator might require certain activities to be implemented by social networking services including reporting buttons, clear terms of reference, codes of conduct, content disclosure, client disclosure, effective terms and conditions of service, transparency reports, trend reporting, etc. These agreed responsibilities will need to be auditable, verifiable and reviewable by the regulator and will require the implementation to be self-regulated on a day-to-day basis with unannounced audits implemented by the regulator.

5 Question 2:
- If the regulator is to be involved in deciding whether individual pieces of content should or should not be removed, should a statutory test be put in place before an appeal can be escalated to the regulator? Please describe any statutory test which you consider would be appropriate.

[Sections 2, 4 & 8 of the explanatory note]

The regulator could receive reports from Irish/European citizens or from any internet user or perhaps restricted to the industry hotline/moderator. If the regulator is implemented to receive reports from internet users in Europe or globally, this would introduce the possibility of the regulator being the target of spurious and an overwhelming volume of requests and it will be difficult to prioritise reports received - with the purpose of prioritising the reports of immediate threat to safety or life in relation to less critical reports requiring action over a less urgent period of time. Any referral to the regulator should first be reported to the specific internet service and/or the industry funded moderator/hotline to review the report and assess the suspect content. The exact nature of the reported suspect content or activity (hate speech, etc) needs to be clearly specified and the report should include the nature of the report. If open reports are permitted to be lodged with the regulator then it will require extra resources for the regulator to identify the likely illegal or harmful nature of the suspect content and to locate the suspected content among a range of other content. If a satisfactory decision is not reached then the content might then be referred to the regulator. A statutory test might include a prerequisite that the report has already been reported to the service provider and/or the industry hotline. Depending on the nature of the reported content it might require that the suspect content has immediate harm to a wider range of persons rather than an individual. Any referral to the regulator should include the resulting decision and explanation received by the service provider or industry hotline. Any investigation needs to be coordinated against possible ongoing investigations by law enforcement to ensure that no ongoing investigations are disrupted.

6 Question 3:
- Which online platforms, either individual services or categories of services should
be included within the scope of a regulatory or legislative scheme?

[Sections 2, 5 & 6 of the explanatory note]

There is a wide range of telecommunications businesses active in the internet marketplace providing from basic internet access providers through the latest evolution of online services which continually expand based on creative ideas and market opportunities. Although there are different positive responsibilities which each organisation in the internet hierarchy can contribute, the internet organisations currently in the spotlight primarily relate to social networking services, video-on-demand services and online gaming services. Since internet related technologies continues to evolve in unpredictable ways it would be a mistake to narrowly define the specific services which need to be addressed. Instead any attempted definition should focus on the broad services offered such as offering services to a wide range of citizens including minors and special needs individuals. It should be possible to start with a narrow remit and as skills and effectiveness improve or as requirements, demands and risks of the market change the remit could be expanded on request of the regulator or by the relevant Minister.

Question 4:
- How should harmful online content be defined in national legislation? Should the following categories be considered as harmful content? Online platforms are already required to remove content which it is a criminal offence under Irish and EU law to disseminate, such as material containing incitement to violence or hatred, content containing public provocation to commit a terrorist offence, offences concerning child sexual abuse material or concerning racism and xenophobia. Are there other clearly defined categories which should be considered?

For example:

- Serious Cyber bullying of a child (i.e. content which is seriously threatening, seriously intimidating, seriously harassing or seriously humiliating)
- Material which promotes self-harm or suicide
- Material designed to encourage prolonged nutritional deprivation that would have the effect of exposing a person to risk of death or endangering health

[Sections 2, 4 & 6 of the explanatory note]

Two issues are often erroneously conflated – 1) illegal online activity and content and 2) harmful content and activity online and are very different issues with significantly different responses. A new category is now being debated in society called “severe harm”. 1) Illegal content needs close collaboration with An Garda Siochana to ensure successful investigations and prosecutions. Much work has been achieved in the current self-regulatory regime where many major global internet companies offer law enforcement portals, training, tools and sometimes joint-investigation-teams (JIT). Of course these activities should be supported and encouraged as technology improves. 2) The difficult challenge is that harmful content is demanding to define and identify independently of the effect caused by suspect content which further requires understanding the impact of the suspected harmful content on the receiver or reader of the suspicious content with specific care for minors or persons with special-needs. It must be assumed that the content
is different from illegal content and activity which is already clearly defined by law – subject to updates and improvements over time. As regards harmful content the two major areas identified as Serious Cyber Bullying and material which promotes self-harm or suicide are pressing issues which should be part of the early mandate of a regulator. In section 4, the consultation paper refers to the legislative framework established by the European Union law under the eCommerce directive. A key element of this directive has been the issue referred in the paragraph about the role of mere conduit and liability for hosting illegal content. The consultation states that “if they are made aware of the illegal content they are required to act expeditiously to ensure its removal form their service”. Previous interpretations internationally have referred to a higher standard of awareness called “actual knowledge” which is used in section 13 of the directive in relation to caching. A huge challenge in this area is to determine that content IS illegal (usually a role for law enforcement and the courts) and to be able to accurately and concisely specify the specific content that is suspect. These two issues can be very difficult for the internet citizen to determine in order to make a service provider “aware” of, or have actual knowledge of, illegal content. The regulator can offer a clear role in ensuring best practice and effective initiatives in this area. There are legal and justifiable reasons why harmful content might be discussed or propagated online since suspicious content depends on a complex range of factors and prior research and knowledge. There is also the problem of identifying suspect content in a world of complex emoji, song lyrics and hidden/obfuscated modern language dialects related to online activities.

Page 4

8 - Question 5:
The revised Directive introduces a definition of Video Sharing Platform Services. Where should the limits of this definition be, i.e. what services should and shouldn’t be considered Video Sharing Platform Services? Please include your rationale and give examples.

[Section 3 of the explanatory note]

The focus of Video Sharing Platform services should only be concerned with internet service providers where a very significant element of the online service IS directly about online streaming of video content including activities such as YouTube, Vimeo, RTE Player, Virgin Media Player, iTunes, etc. However, internet services which provide incidental or supplemental online video services such as WhatsApp, Facebook, LinkedIn, Skype, Snapchat, etc will provide a greater challenge since these services are also sometimes abused for illegal and harmful activities. These latter services would need to be under the remit of the proposed regulator as they relate to possible illegal or harmful use.

9 - Question 6:
The revised Directive takes a principles based approach to harmful online content and requires Video Sharing Platform Services to take appropriate measures to protect minors from potentially harmful video content, the general public from video containing incitement to violence or hatred and certain criminal video content. It also requires that Ireland designate a regulator to oversee the ongoing implementation of these measures.

Given this, what kind of regulatory relationship should there be between a Video Sharing Platform Service established in Ireland and the Regulator?
The regulator would need to have a working relationship with the VSPS established in Ireland with the ability to review and report on current practices and to require certain capabilities to be put in place at the VSPS. It is not clear which services are within the capabilities of the VSPS to implement without changes in Society. For example, an age verification system would need the ability to legally determine and profile the age of users using real-world data bases such as passports, birth certificates, etc and would have a major challenge in the balance between the rights of a child and the rights of their guardians. E.g. where would the balance rest between the rights of a minor to information about sexuality or drugs against the rights of society to restrict access to sexual or drug related explicit content.

10 Question 7:
- On what basis should the Irish regulator monitor and review the measures that a Video Sharing Platform Service has in place, and on what basis should the regulator seek improvements or an increase in the measures the services have in place?

There should be a scale of sanctions: a) Ability to request disclosure and demonstrate current policies, practices b) Review and require improved staff training when required c) Transparency Reports for public dissemination d) Ability to audit current activities e) Public naming sanction f) Issues notices that require compliance g) Issue fines for inappropriate or inadequate responses h) Revoke permission to offer/operate a service in extreme situations i) Revoke licence to operate in extreme situations

11 Question 8:
- The revised Directive closely aligns the rules and requirements for television broadcasting services and on-demand audiovisual media services. Given this, what kind of regulatory relationship should there be between an on-demand audiovisual media service established in Ireland and the relevant Irish regulator? In addition, should the same content rules apply to both television broadcasting services and on-demand audiovisual media services?

No comment.

12 Question 9:
- Should Ireland update its current content production fund (Sound & Vision fund currently administered by the BAI from licence fee receipts) to allow non-linear services to access this fund? Should Ireland seek to apply levies to services which are regulated in another EU Member State but target Ireland in order to fund or part-fund an updated content production fund?

No comment.

13 Question 10:
- The United Nations Special Rapporteur on the promotion and protection of the
right to freedom of opinion and expression has previously raised concerns regarding the National Legislative Proposals under Strand 1. How can Ireland balance the fundamental rights of all users, e.g. the right to freedom of expression, including those affected by potentially harmful online content and those creating said content, in pursuing the further regulation of harmful online content?

[Section 2, 4, 5, 7, & 8 of the explanatory note]

The European Court of Human Rights has often reiterated that freedom of speech is not only for content which is positive and good but also speech which is provocative, challenging and possibly unpleasant (note 1). It is important that any intervention in the marketplace does not unreasonably impact on freedom of speech in democratic societies. In order to understand the complexities of this issues, I would refer the reader to work completed by the Mandola (Monitoring and Detecting Online Hate Speech) project funded by the European Commission which I participated in on the definitions of hate speech across Europe and specifically the work done on the Final report: Definition of illegal hatred and implication where a comparative analysis covering ten E.U. member States identified a wide heterogeneity and complexity of legislations targeting hate speech, which has consequences on the determination of an acceptable definition of illegal online hate speech (the notion of “definition of illegal hate speech” being understood as referring to the identification of hate speech that is currently illegal). This analysis leads to propose both a detailed and shorter definition of illegal hate speech covering the ten E.U. member States that have been studied, which - together with a short overview of penalties and problems. Note 1 Subject to paragraph 2 of Article 10, it is applicable not only to “information” or “ideas” that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no “democratic society”. https://en.wikipedia.org/wiki/Handyside_v_United_Kingdom

Question 11:
- How can Ireland ensure that its implementation of the revised Directive under Strand 2 and any further regulation of harmful online content under Strand 1 fits into the relevant EU framework for the regulation of online services, including the limited liability regime for online services under the eCommerce Directive? [Section 2, 4, 5, 6, 7, & 8 of the explanatory note]

As President of the European Internet Service Provider Association (EuroISPA) in 2001 I represented over 800 ISP’s across Europe during the debates with the European Commission and Parliament on the eCommerce Directive. The issue of limited liability was always an important issue which has supported the development of internet services over the last two decades. The limited liability protects internet service providers who offer intermediary internet communications services to end-users when these same end-users behave in an illegal manner without the actual knowledge of the internet service provider. However, this liability is limited and will not always protect the intermediary. In most democratic jurisdictions, Internet Service Providers are not permitted to intercept or monitor internet communications unless requested and authorised by law. The issue of actual knowledge also states that the Internet Service Provider must take action when they gain actual knowledge of illegal content or activity using their internet
services. A key element in this responsibility and liability is based on the legal understanding and interpretation of what constitutes actual knowledge. Early self-regulatory regimes performed an exclusively reactive function where suspect content/activity is reported as suspect and is then reviewed by independent organisations with extensive expertise on illegal and harmful content to determine where the content is located on the internet and whether the content is likely to be illegal under the appropriate national law. The decision is then communicated to the relevant internet service for action. Once such notice has been issued, it is expected that actual knowledge of illegal activity has been given to the hosting provider – removing the protections received under the eCommerce directive. Delays in removing or blocking content can then be a legal problem for the internet service provider. Recent debates in society relate to the possible role of third party organisations or the internet service provider to perform enhanced reactive evaluations through prudent, minimal, reasonable, mostly automated proactive assessment or moderation or profiling of online activities to identify potentially illegal or harmful content or activity. These activities need careful balance in democratic societies to protect free speech and rights to communicate without interception or monitoring with the rights of individuals to be free of harassment and victimization and access internet services without fear or unreasonable risk. The significant challenge therefore is to balance competing rights as outlined in the range of historical judgements issued by the European Court of Human rights. There is no simple solution to this balance except to understand that expertise, tools and knowledge continues to grow and it is important that all stakeholders work together to ensure a safer internet.

Question 12:
Potential options for regulatory structures to progress the regulation of the four streams are identified in the explanatory note accompanying these questions. These options include:

- Restructuring the Broadcasting Authority of Ireland as a Media Commission responsible for the four strands

- Two regulatory bodies. Assigning the responsibility for editorial services, e.g. on-demand audiovisual media services, to a restructured BAI and creating another regulatory body with responsibility for non-editorial online services, e.g. Video Sharing Platform Services.

Is one of these options most appropriate, or is there another option which should be considered?

[Section 5 of the explanatory note]

There is no significant preference for either strategy as long as the internet focused regulation has its own focus, clear budget and responsibilities especially in the embryonic phase of activity. There is an advantage is sharing complimentary skills between traditional broadcasting regulatory skills and experiences and newer evolving cyber skills.

Question 13:
How should the chosen regulatory structure or structures be funded given the various categories of services which are to be regulated?
Funding is a challenging issue. The role of the regulator is to benefit society at large and as such should benefit from significant government funding – especially in the early years. However, it is clear that some internet businesses are currently generating significant income and profits from their services and should contribute to a safer internet. It might be possible to consider a cost sharing model which requires some supporting funds to be collected from Internet Service providers in the Irish market. However, it should be acknowledged that the impact of regulation could be a major barrier to entry for new internet business services as a result of both contributing to the running costs of a regulator and also by the significant burden to manage the regulatory requirements in terms of equipment and personnel. Such direct and indirect costs and potential negative impact against novel internet business models could have a substantial chilling effect on foreign direct investment in the Irish market and will certainly become a comparative issue across the European area. It will have a particular chilling effect on newer business models and will be a barrier to entry for those businesses. This might be addressed by offering lower contributions and regulatory requirements at low customer and profit levels which increases as income and customer volumes increase. In addition, the skills and equipment required to operate in the cyber safety and security space are scarce and expensive and are in high demand across the world. This will bias towards higher setup and running costs associated with the regulator.

17 Question 14:  
- What functions and powers should be assigned to the relevant regulator to allow them to carry out their monitoring and enforcement role (some examples have been provided in Section 8 of the explanatory note)? In addition, should these functions and powers differ between regulation for Video Sharing Platform Services under the revised Directive under Strand 2 and regulation adopted at a national level under Strand 1? Please include your rationale and give examples.

18 Question 15:  
- What sanctions should be available to the relevant regulator to apply to a service that does not comply with its obligations? Such sanctions may include
  - The power to publish the fact that a service is not in compliance,
  - The power to issue administrative fines,
  - To issue interim and final notices to services in relation to failures of compliance and the power to seek Court injunctions to enforce the notices of the regulator,
and,

- The power to apply criminal sanctions in the most serious cases.

Are there any other sanctions which should be considered? please provide your reasoning as to why the regulator should have recourse to a particular sanction. 
[Sections 2, 4, 6, 7 & 8 of the explanatory note]

First 3 the Q14 The final sanction should require law enforcement investigations, prosecution and courts to reach a decision on criminal liability especially as they relate to legal persons and persons in leadership responsible roles in legal entities. This might be something that could be added later.

19 Question 16:
- Given that the revised Directive envisages that a Video Sharing Platform Service will be regulated in the country where it is established for the entirety of the EU it does not envisage that the relevant regulator would assess individual complaints. However, the revised Directive requires Ireland to put in place a system of mediation between users and Video Sharing Platform Services. Given that such a system would be in place on an EU-wide basis should thresholds apply before an issue could be brought before this system? If so, then what thresholds would be most appropriate?
[Sections 2, 4, 6, 7 & 8 of the explanatory note]

Offering a mediation service for users across the EU will require language support. It would be best if such complains are first reported to a national regulator who would then refer the matter for mediation to the Irish regulator. This would permit early detection of minor or resolvable issues and higher quality referrals to the Irish based regulator.