TO: **COMMUNITIES, HOUSING AND PLANNING POLICY BOARD**

ON: **20 AUGUST 2019**

REPORT BY: **DIRECTOR OF COMMUNITIES, HOUSING AND PLANNING SERVICES**

HEADING: **UK GOVERNMENT ONLINE HARMS WHITE PAPER – CONSULTATION RESPONSE**

1. Summary

1.1 The UK Government launched the consultation on its Online Harms White Paper in April 2019. This set out the government's plans for a package of online safety measures that will also support innovation and a thriving digital economy.

1.2 The White Paper proposes establishing in law a new duty of care towards users, which will be overseen by an independent regulator and the consultation aimed to gather views on various aspects of the government's plans for regulation and tackling online harms.

1.3 The final date for submissions to the consultation was 1 July 2019. A response from the Council was submitted within the timescales set by the UK Government and is attached as Appendix 1.

1.4 The consultation response submitted on behalf of Renfrewshire Council welcomes the opportunity to respond to the white paper and is supportive of the approach and proposals that are outlined to strengthen the process for reducing on-line harm to vulnerable people. In particular, the response acknowledges the challenges involved in taking forward this agenda and is in favour of increased regulation in relation to the expectations and responsibilities placed on companies operating online services; and to the creation of a proportionate and supportive enforcement approach that will allow the digital economy to develop while protecting vulnerable service users.

2. Recommendations

2.1 It is recommended that the Communities, Housing and Planning Policy Board:

(i) notes the consultation on the UK Government Online Harms White Paper; and

(ii) homologates the Council's submitted consultation response as detailed in Appendix 1 to this report.

---

3. Background

3.1 The Online Harms White Paper set out the government's plans for a package of online safety measures that will also support innovation and a thriving digital economy. This package comprises legislative and non-legislative measures and will make companies more responsible for their users' safety online, especially children and other vulnerable groups.

3.2 The White Paper proposes establishing in law a new duty of care towards users, which will be overseen by an independent regulator. Companies will be held to account for tackling a comprehensive set of online harms, ranging from illegal activity and content to behaviours which are harmful but not necessarily illegal.

3.3 This consultation aimed to gather views on various aspects of the government's plans for regulation and tackling online harms, including:

- the online services in scope of the regulatory framework;
- options for appointing an independent regulatory body to implement, oversee and enforce the new regulatory framework;
- the enforcement powers of an independent regulatory body;
- potential redress mechanisms for online users; and
- measures to ensure regulation is targeted and proportionate for industry.

3.4 The consultation response submitted on behalf of Renfrewshire Council welcomes the opportunity to respond to the white paper and is supportive of the approach and proposals that are outlined to strengthen the process for reducing on-line harm to vulnerable people. In particular, the response acknowledges the challenges involved in taking forward this agenda and is in favour of increased regulation in relation to the expectations and responsibilities placed on companies operating online services; and to the creation of a proportionate and supportive enforcement approach that will allow the digital economy to develop while protecting vulnerable service users.

Implications of the Report

1. **Financial** – None

2. **HR & Organisational Development** – None

3. Community Planning

Renfrewshire is Safe – The consultation and regulatory body being put in place should allow all Renfrewshire residents including vulnerable groups to be better educated, supported and protected by the Renfrewshire Community Safety Partnership.

4. Legal – None

5. Property/Assets – None

6. Information Technology – There may be a requirement for Renfrewshire Council as a provider of online services to provide evidence of compliance with the new duty of care to the newly appointed regulator.

7. Equality & Human Rights - The government's plans for a package of online safety measures provides an opportunity to strengthen and reinforce the need to consider equality in the design and delivery of online services for users' safety online especially vulnerable groups and children who share a relevant protected characteristic and those who do not.

8. Health & Safety – None

.

9. Procurement – None

10. Risk – None

11. Privacy Impact – None

12. CoSLA Policy Position – None

13. **Climate Risk -** None

List of Background Papers

Background Paper 1. Online Harms White Paper – UK Government
https://www.gov.uk/government/consultations/online-harms-white-paper

The foregoing background papers will be retained within Communities, Housing and Planning Services for inspection by the public for the prescribed period of four years from the date of the meeting. The contact officer within the service is the Communities and Regulatory Manager.

OR
13 August 2019

Author: Oliver Reid, Head of Communities and Public Protection.
Email: oliver.reid@renfrewshire.gov.uk

Appendix 1

Question 1: - This government has committed to annual transparency reporting. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

We agree that more needs to be done to build a culture of transparency, trust and accountability across the industry and suggest annual transparency reporting is available 'at a glance' as a summary in appropriate language and strong graphics, presented in a clear way and easily available online to reach a wider audience. We believe that large companies should be required to dedicate a percentage of their advertisement time to online safety and transparency awareness.

We recommend that it would be good to identify timescales for companies to respond to the regulator, strengthening the powers given to the regulator and force the companies to take cognisance of reporting and transparency.

Question 2: - Should designated bodies be able to bring 'super complaints' to the regulator in specific and clearly evidenced circumstances?

We agree with the proposal and the need for oversight of complaints, such as an independent On-line Ombudsman who can pursue companies not addressing the complaints.

We seek clarification on the definition of who is/are 'designated bodies', and if there will be another way of raising complaints with an independent third party?

We recommend further consideration is given regarding customer complaints procedures currently in place or provided by companies which may not be easy to access and use, the customer may have concerns about going directly to the company with a complaint or may not trust the company to listen. Could a mechanism be put in place to raise all company complaints and resolutions with the regulator in real time instead of waiting for an annual report. The regulator could undertake spot checks and focus on unresolved complaints in a specific timeframe or those identified as high risk, encouraging and improving transparency, accountability and tracking

Question 2a: - If your answer to question 2 is 'yes', in what circumstances should this happen?

We suggest a threshold or points system is established where violations or concerns have a value and when the value reaches a certain threshold a 'Super Complaint' can be opened against the company, that is, where a company or organisation have a history of violations that would amount to justifying a 'Super Complaint' being made

Examples may include;

- where a complaint has not been resolved in a timely manner,
- where a complaint is common and being repeated,
- where a complaint is from a group or large number of individuals,
- complaint is identified as high risk in terms of online safety

Question 3: What, if any, other measures should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

We believe that companies need to provide clear and concise guidance to allow users to complain, should they remain dissatisfied an appeal/escalation process should be built in.

Consideration should be given to establishing new innovative online tools and services available to users which make it easy and quick for users to report violations or harmful content, for example a browser extension could be developed that takes a 'snap shot' recoding an image of webpage being reported along with the website code, uploading it to reporting systems (image does not download onto users pc)

We recommend and suggest developing an online portal for logging these complaints with the regulator or an independent party. The portal may encourage the use of contacting the company first providing a reference number which can be used to log a concern with the regulator. It is essential that a help and advice line is available for those not comfortable with online systems or looking for immediate support and guidance

Question 4: - What role should Parliament play in scrutinising the work of the regulator, including the development of codes of practice?

We believe that Parliament should be key in reviewing and scrutinising the work of the regulator but the development of the codes of practice should be left to the independent body.

Based on our understanding of the White Paper we believe there may be a need for a Scrutiny Sub Committee to be established to oversee the regulator. Our response is also based on a view that Parliament and MPs will have access to information and documents that are not available to others, therefore this should influence the regulator and codes of practice

We recommend that Parliament should release statements or reports pertaining to the codes of practice that are developed providing a stronger message that these codes of practice are supported and endorsed by Parliament. It is essential that clarity is provided on the codes of practice to ensure that codes are not open to misinterpretation. Codes of practice may require upskilling that could be provided via online training or required certification to prove that you understand them.

Question 5: - Are proposals for the online platforms and services in scope of the regulatory framework a suitable basis for an effective and proportionate approach? 98 Online Harms White Paper

We seek clarification regarding the approach of specific monitoring of communication outlined in paragraph 3.12, how will the regulator ensure;

- that companies will use an effective and proportionate approach, with appropriate safeguards
- development of appropriate safeguards to ensure that the monitoring is legal and justified, particularly as the monitoring will likely be conducted by a private company rather than a public body performing statutory responsibility
- that the private company can balance the interest of the individual, the public and the companies' own interests fairly and proportionately and
- how will care be taken to ensure individuals' rights to privacy and freedom of speech are not encroached upon

Question 6: - In developing a definition for private communications, what criteria should be considered?

We believe that private communication should be defined as any communication that appears to the user to be private, i.e. sending a direct message to a named person, whether it is a private message, email or instant message. Communications behind a password protected website or file that cannot be accessed without passwords/credentials or specific knowledge such as connecting to an IP address and port number is private communication.

It is our view that expectation of privacy should be a fundamental criterion in developing a definition for private communications. The mindset and belief of the individuals entering into and continuing to take part in the communications should be taken into account. As should the extent to which the companies have explained and taken steps to ensure that the individuals understand that such a private and public communications distinction can arise on their platforms.

Question 7: - Which channels or forums that can be considered private should be in scope of the regulatory framework?

We suggest that as part of this paper a discussion is required for channels and forums to assess what should be in scope. Private messaging is clearly a channel that is being used for activities that should be targeted. This could include anything behind a password or that has a security protocols that create a private-like environment, such as private video game servers and Teamspeak servers without passwords but require knowledge specific IP address and port number.

However, there already exists a legal framework for the interception of communications in very narrow circumstances. The Article 8 infringement involved in monitoring such a private space requires the scrutiny to be proportionate and that is only likely to be the case for CSEA or national security issues

Question 7a: - What specific requirements might be appropriate to apply to private channels and forums in order to tackle online harms?

There are significant challenges and it will be impossible to monitor and regulate any small private web server or service server (voice over IP, gaming etc) without impacting encryption and making the UK unable to compete in the global online market. Servers outside of the UK cannot be held to UK law, so any new online safety body would only be able to regulate UK based servers.

We also believe that modern technological advances would need to be used to identify key descriptors, behaviours, words that could identify issues and an easy way of reporting online harms and sharing evidence while using a private channel.

Question 8: - What further steps could be taken to ensure the regulator will act in a targeted and proportionate manner?

We suggest consideration is given to creating a partnership with another organisation such as OFSTED to spot check/audit randomly selected open and previous cases which will help to ensure the response is proportionate and the targeting of new cases has been appropriate and justified.

Developing a clear strategic and operational plan could assist the Regulator to highlight what will be done. The Parliamentary oversight/scrutiny would assist in ensuring proportionality. The principles of Better Regulation have been mentioned and require to be followed: Transparency, Proportionality, Accountability, Targeting and Consistency.

Further consideration can be given to using algorithms/automation to identify patterns of behaviour or to flag risk areas to help understand where the highest or most harmful online safety issues occur or who is at most risk.

Question 9: - What, if any, advice or support could the regulator provide to businesses, particularly start-ups and SMEs, comply with the regulatory framework?

We believe that there are many challenges when it comes to implementing this framework for smaller businesses who may not have the staff or technology to effectively monitor this kind of online service/online presence. Effective and easy to use reporting tools available to users would be the most effective way to regulate SMEs and start-ups.

Our view is that anyone who is designing anything to do with any form of digital services should be obligated to design security in at the start and to make the strictest privacy controls the default setting instead of the least. Therefore, consideration could be given to including the level and type of support for start-ups and SMEs in any Strategic and Operational Plans that will be developed to comply with the regulatory framework

Question 10: - Should an online harms regulator be:

(i) a new public body, or

(ii) an existing public body?

We recommend that a new public body with sole oversight of this issue should be established that understands the complexities of online harm and online communications. A modern body with extensive knowledge of all aspects of internet culture, and an understanding of the complexity of regulating a global space like the internet. Online safety is too large a remit to apply existing standards and regulations and requires specific development to be effective as a body. Existing public bodies may bring established, or traditional, methods to the table that do not work in online space.

Question 10a: - If your answer to question 10 is (ii), which body or bodies should it be?

We believe it should be a new body

Question 11: - A new or existing regulator is intended to be cost neutral: on what basis should any funding contributions from industry be determined?

Our view is that Industry should be required to pay a membership fee in order to operate in the UK, likely based on the size of the organisation. Fines would also be a potential funding source and again should be based on the size of the company.

Funding contribution will also depend on the resource requirement of the Regulator. This area is simply going to grow, and people change behaviours, therefore the Regulator needs to grow with it. Contributions should potentially be proportionate to the time the Regulator spends on that company i.e. if they spend a lot of time of a single company, they need to pay more (similar to Fees for Intervention by the Health and Safety Executive).

Question 12: - Should the regulator be empowered to

(i) disrupt business activities, or

(ii) undertake ISP blocking, or

(iii) implement a regime for senior management liability?

What, if any, further powers should be available to the regulator?

We believe that the Regulator needs full power to be able to get companies to comply. This will be challenging legally, especially for companies out with the UK

Disrupt business activities and Implement a regime for senior management liability. Blocking at ISP level may violate the goal of having a "free and open internet". If an ISP is seen to facilitate activities in violation of the new regulations, then they would also be subject to business disruption and senior management liability.

Public reporting on those who break the codes of practice and where proven that a company is not taking their obligations seriously.

Question 13: - Should the regulator have the power to require a company based outside the UK and EEA to appoint a nominated representative in the UK or EEA in certain circumstances?

We suggest that if a pre-agreed threshold had been met or a major violation had taken place then the body should request a representative, and if one is not supplied then the new body should work with international bodies to further the issue.

A nominated representative in the UK or EEA may be beneficial in allowing companies to better understand and maintain contact with a website supplier.

Question 14: - In addition to judicial review should there be a statutory mechanism for companies to appeal against a decision of the regulator, as exists in relation to Ofcom under sections 192-196 of the Communications Act 2003?

We agree that independent bodies (to be identified) could review appeals and manage the process, or a specific appeals department of the new body should be formed to ensure fairness for the Companies

Question 14a: - If your answer to question 14 is 'yes', in what circumstances should companies be able to use this statutory mechanism?

We agree that companies should be able to use statutory mechanism when companies feel aggrieved with the sanctions put in place, this could be considered as a cost neutral i.e. if they lose the appeal they pay the appropriate costs.

Question 14b: - If your answer to question 14 is 'yes', should the appeal be decided on the basis of the principles that would be applied on an application for judicial review or on the merits of the case?

Our response to 14 is based on our belief that if there is supporting evidence to counteract the claims against companies and there should be consideration on the merits of the case.

Question 15: - What are the greatest opportunities and barriers for

(i) innovation and

(ii) adoption of safety technologies by UK organisations, and what role should government play in addressing these?

Our response is as follows;

i) innovation

Any unnecessary intervention into the internet and how it is monitored may affect the goal of providing a "free and open" internet to the UK public. Discourse online could be affected, and new and innovative apps and websites could find themselves in violation of new regulations, potentially stifling the UK as a tech industry growth centre. Other considerations to industries such as the financial tech industry, healthcare, medical science, defence etc. should be taken, as maintaining secure and private communications are vital for these industries to operate in an effective manner. Upskilling to enable informed decisions throughout the innovation design process. A safety checklist to act as a guide or reference point?

Opportunities for innovation could lie in establishing a mature online safety industry in the UK which could act as advisory bodies on a global stage.

ii)adoption of safety technologies by UK organisations

the UK can become a global leader in Online Safety by developing a framework and new independent body that other nations will look to for guidance and potentially set up bodies of their own using the frameworks developed by the new body. Developers, manufacturers and resellers still do not see cyber security as their responsibility and instead transfer this to the customer who is rarely skilled enough to be able to really help keep themselves or their family safe from cyber based threats.

Question 16: - What, if any, are the most significant areas in which organisations need practical guidance to build products that are safe by design?

We believe implementing internet safety standards without compromising network and information security.

Developing a star rating for quality of cyber security might help to give companies a push towards building products that are safe by design, so people know they are buying something that already has good security-built in.

Question 17: - Should the government be doing more to help people manage their own and their children's online safety and, if so, what?

We believe that the government could do more to address online harm targeted at people at risk of self-harm, suicide, or eating disorders. Available materials that promote these types of behaviours and sites that give "tips" in order for people to harm themselves should be scrutinised and regulated with far more intensity than appears to be the case at present.

These risks are present for both children and adults alike. Adults at risk of harm need the reassurance that government is not focused solely on safeguarding children but also takes their safety seriously

To ensure consistency of prevention and intervention messages government should provide Easy Read and accessible formats for education and awareness raising. It should not be left to or expected that businesses will produce all of their own materials. Businesses could be given templates or base materials, which they could then individualise for their use.

Embedded within the policies should be recognition of existent safeguarding pathways, like Child (CP) and Adult Protection (ASP). The regulator may have own referral process when cyber harm is identified in future, but we do not want this to overshadow the need for referrals to be made under CP or ASP, if relevant criteria are thought to be met.

We believe the government should be considering actively implementing this as part of the school curriculum. When children are receiving lessons on the use of ICT, this should go hand in hand from an early age. This will allow future generations to be clear both as children and into adulthood.

Careful consideration should be given if parents should be legally responsible for their children online under a certain age, with guidelines available for parents. Schools should reinforce lessons taught at home regarding internet safety, to reinforce a societal attitude to how to act online and how to mitigate risk, similar to how primary school aged children are taught about crossing the street or riding a bike on the road in a safe way while in a school environment. Schools and local councils should support parents by providing information and requiring parents to sign a form which demonstrates their understanding about their child's safety on the internet while visiting a school or public building to use online services.

For the average person, they have to search to find out information about being safe online and even then, often don't know what they are looking for. Also, many adults still think of 'digital' as being a PC. Today's younger generation may be doing things online from many other devices. Public information advertising should be used to make people aware of things they need to consider and how to find out more,

Question 18:- What, if any, role should the regulator have in relation to education and awareness activity?

We believe the regulator should provide case studies, guidelines to schools and appropriate organisations that work with children and/or teenagers. Local authorities should offer advice as part of their offering to support individuals with additional needs or who may be vulnerable

The regulator should have a significant role in the education of adults on how technology, digital services and online activity can do real harm to people and families

The regulator should have a role to inform the content of training programmes and to evaluate the effectiveness of programmes, promote which interventions are most successful. To develop a self-assessment tool or survey to help understand the national online safety skills / awareness baseline and to benchmark

We strongly recommend the regulator needs to acknowledge that some adults are just as vulnerable to cyber harm as children. We must ensure that individuals who are vulnerable (through ill health; mental or physical infirmity; or disability) are equally recognised and safeguarded through any new regulation. We think that it is imperative that the regulator take the lead in not just promoting but requiring that Easy Read and accessible-format materials be produced and disseminated widely in relation to cyber harm education and awareness.

The regulator needs to understand that consistent messages of prevention and intervention are important; We want to ensure that recognition of cyber harm and reporting through new channels does not detract from people's understanding and use of current referral pathways for protecting adults and children.