A Summary - Online Harms White Paper

Online Harms: this is behaviour online which may hurt a person physically or emotionally. It could be harmful information that is posted online, or information sent to a person.

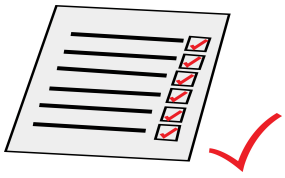
White Paper: this is the second step to writing a new law. It sets out plans for new laws or changes to the existing law.

1. The government wants the UK to be the safest place in the world to go online. The government also wants the UK to be the best place to start and grow a **digital business**.

Digital business: this is a way of doing business online using technology.

There is a lot of illegal and hurtful information online. People in the UK and the rest of the world are worried about online harm.

For these reasons, we think that the **digital economy** needs a new **regulatory framework** to make sure that people are safe online.



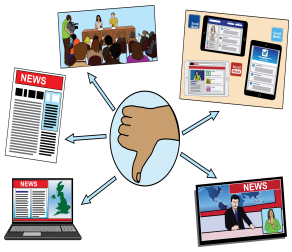
Digital economy: this means everybody that does business online and using technology.

Regulatory framework: here, this means rules and laws so that people and companies know what their rights and responsibilities are.

This will make sure people feel safer and more confident online. It will also set out clearly what we expect from companies.

The problem

2. There is a lot of illegal and harmful information and activity online. People in the UK are worried about what they see and experience on the internet. This information can be a threat to the safety of the UK and to the safety of our people, especially our children.



Online platforms can be used for abuse and bullying too. They can also be used to go against our **democratic values** or to stop proper **debate** from happening.

Online platforms: this means sites or places online where you can buy and sell things or share information.

Democratic values: these are our ways of thinking, such as everyone being free, everyone being treated equally and fairly and **freedom of speech**.

Freedom of speech: this means that people are able to say what they think without being scared or punished for thinking that way.

Debate: this means talking about an issue and looking at the different sides of the argument.

Some information online can be very harmful for children. People are more and more worried about how this affects their **mental health** and wellbeing.

Mental health: this means how we think and feel. For example, someone who is often sad or worried, may have poor mental health.

3. Terrorist groups use the internet to spread information that is used to **radicalise vulnerable people**. They also use the internet to spread information which is used to support or carry out terrorist attacks. There are also examples of terrorists filming attacks live on social media.

Radicalise: this means that a person starts to take on values and ideas that are very different from most people's values and ideas. For example, supporting violence.

Vulnerable people: this means people who may be at risk of abuse.

Child sex offenders use the internet to watch and share child sexual abuse. They also use it to watch videos, **groom children** online, and even **live stream** abuse.

Child sex offenders: these are people that carry out sex crimes against children.

Groom children: this is when a person talks to a child, gives them gifts and prepares them for a meeting or to be abused.

Live stream: this is when something is put on the internet at the same time as it is being recorded.

4. There is also a real danger that some people use information that is not true, to go against our democratic values. **Social media platforms** use **algorithms** which sometimes mean you only see one point of view and not all sides of an argument.

Social media platforms: this means things like Facebook, Twitter or other sites where you can share information online and build a network.

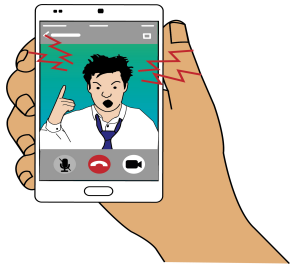
Algorithms: these are, calculations, instructions and rules that computers and other technologies use to make decisions about what people see online.

This can mean that people don't hear different voices and opinions and only see one side of the story. It means that information that is not true can spread. It means that people may not see the other side of the story, or they may not see facts that prove some information is not true. It can also mean that people think that what they see on their social media is believed by many more people than it actually is.

5. Different gangs can use social media to spread **gang culture** and the use of violence. Social media can also be used for selling weapons illegally to young people. This can lead to more violence, such as knife crime, on British streets.

Gang culture: here this means sharing values that gangs may have, such as using violence.

Other behaviour and information online can cause serious harm, even if it is not illegal in all cases. The internet can be used to **harass**, bully or **intimidate**. This is especially true for people in vulnerable groups or in **public life**.

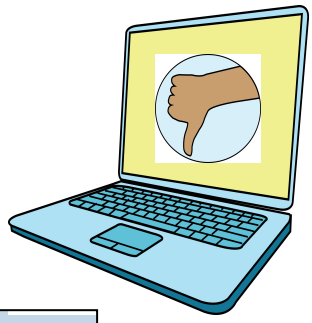


Harass: this is when someone feels scared or worried because a person or a group of people will not leave them alone.

Intimidate: this may be when someone feels scared or worried because a person or a group of people will not leave them alone or are putting pressure on them to do something that they don't want to do.

Public life: this means people that are known and seen out in public. This could be someone famous.

Young adults or children may also see information that is harmful to them, such as information about how to **self-harm** or about how to **commit suicide**. This information can have really serious and harmful results.

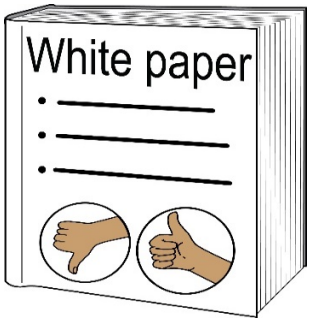


Self-harm: this is when a person hurts themselves.

Commit suicide: this is when a person kills themselves.

There are also new challenges coming up. For example, online services that are made so that it becomes hard to stop using them. There are also challenges around people being on their screens too much.

Our response: this means how we plan to deal with these problems



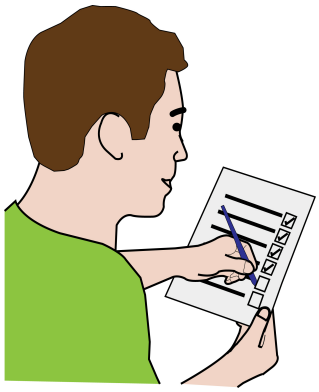
6. This White Paper sets out a plan of action to deal with information or activity that harms people, especially children. It also sets out a plan of action to deal with information or activity that puts our way of life in the UK at risk.

This can include:

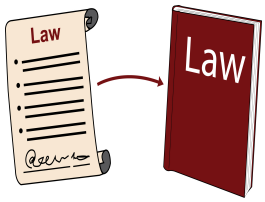
- Being a threat to the safety of the UK,
- Being a threat to our rights and responsibilities,
- Being a threat to **integration** in the UK

Integration: this means making sure different people and cultures can come together and take part in society in an equal way.

7. There are already a number of different things that aim to deal with these problems. Some of these things companies can do by choice and others are things that they must do. However, companies have not gone far enough or fast enough to keep UK users safe online. Also, different companies have dealt with these problems in different ways. This means that they have not been able to keep UK users safe online.

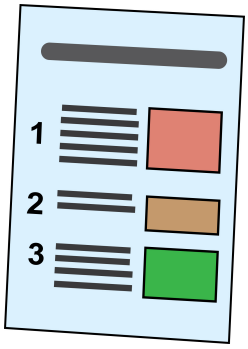


8. Many of our **international partners** are also working on new laws and rules to deal with online harms. However, none of them have put in place a regulatory framework that deals with as many online harms as the new laws will.

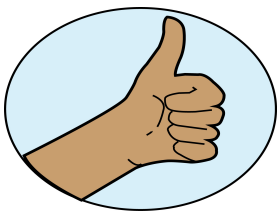


> **International partners:** this means other countries around the world working together with the UK.

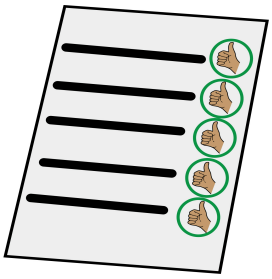
The UK will be the first country to do this and set out a regulatory framework that is:



- Coherent: this means a clear way of doing things
- Proportionate: this means the right level of reaction when doing things.
- Effective: this means something that is done well and works well.



At the same time, we still wish to see a free, open and safe internet.



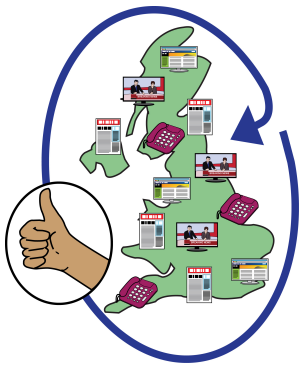
9. The UK is a world leader in new technologies. We want to bring in rules in a way that keeps us leading in this area.

We also want technology to be a part of solving the problem. Our ideas will help make the technology safety **industry** bigger in the UK. We also put forward ways of helping internet users to deal with their own safety online.

> **Industry:** this is an area of business and it includes all of the companies working in that area.

10. The UK is known to be a world leader in pushing for ways of making online safety better. Dealing with harmful information and activity online is one part of a bigger plan for the UK. The plan also includes:

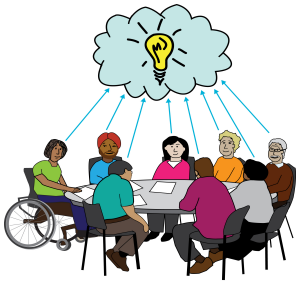
- Keeping personal information safe online
- Supporting competition for online businesses
- Pushing for online design to be responsible.



11. We want to see:

- A free, open and safe internet
- **Freedom of expression** online

Freedom of expression: this means the right to say what you think.



- Companies taking steps to keep their users safe. Also, a place where crime, terrorism and **hostile foreign state activity** is not spread on the internet.

Hostile foreign state activity: this is something done by another country that could be a threat to the UK.

- Rules for the internet that stop people from carrying out harmful behaviour

- The UK as a place where online business can do well. Also, a place where businesses work to find new ways of making the internet safer.

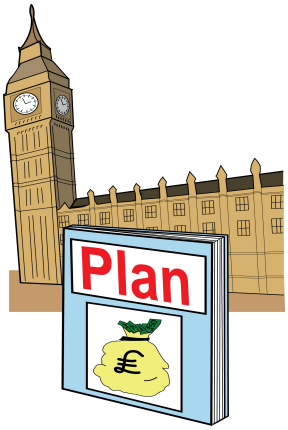
- People who understand the risks of online activity. People who speak out about behaviour that is harmful and know how to access help if they experience online harm – making sure children have extra protection.

- A group of countries from all around the world, working together to take steps to keep people safe online.

- People being able to feel confident and trust in online companies and services again.

Making things clear for companies

12. Growing worries about online harms have led to people asking governments and technology companies to take more action. One of the big reasons for this is that big companies now have more power and control and their sites are now more like public spaces. Some companies now see that they have a responsibility to keep to rules written by countries like the UK.



13. The new regulatory framework that this White Paper talks about will set clear rules to help companies make sure users are safe. At the same time, it will protect freedom of expression.

This is especially important when looking at information or activity that is harmful but not criminal. It could be harmful to children or other vulnerable users. The regulatory framework will push for a culture of companies always working to make things better. It will push companies to make and share new technology to deal with these issues.

14. It will also make things clearer for different businesses of all sizes that will be affected by this regulatory framework. Even if their services do not have a high risk of harm it will help them to understand and meet their **duties**.

> **Duty or duties:** this is something that must be done by a person or organisation. It is usually something that must be done by law.

A new regulatory framework for online safety

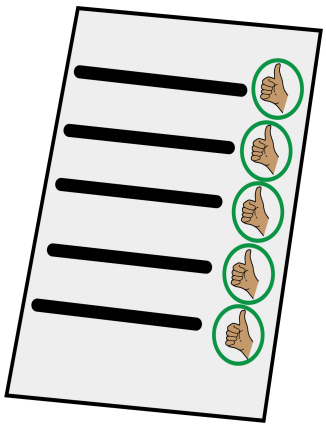
15. The government will put in place a new **statutory duty of care** to make companies take more responsibility for the safety of their users. It will also make companies deal with harm that is caused by information or activity on their sites.

> **Statutory duty of care:** this is a duty in law. It means that an organisation must show how it takes care of the people that use its services.

16. An **independent regulator** will make sure companies meet this duty of care.

> **Independent regulator:** this is an organisation that checks that rules are being kept to. It is independent because the organisation is separate from the Government and is not made up of people from digital companies either.

17. All companies that fall under this regulatory framework will need to be able to show that they are meeting their duty of care. **Terms and conditions** will need to be clear and accessible. This means for children and other vulnerable users as well. The regulator will decide how well these **terms and conditions** are kept to.



> **Terms and conditions:** these are the important rules and information that a person must keep to in an agreement or contract. A contract is an agreement by law.

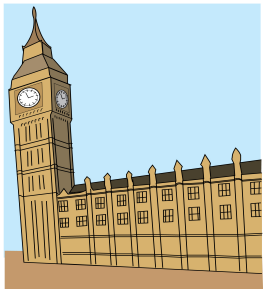
18. The regulator will have a number of powers to take action against companies that do not meet their duty of care. This may be a power to charge big **fines** or a power to make senior managers take responsibility for not meeting their duty of care.

> **Fine:** this is money that a person or organisation must pay if they do not keep to the rules.

19. Companies must meet their new duty by law. The regulator will set out how to do this in **codes of practice**. If companies want to meet this duty in a way that is not set out in the codes, they will have to explain to the regulator how they will do this.

> **Code of practice:** this is a guide about what people and organisations should do to keep to a law.

20. The Government will have the power to tell the regulator what goes in the code of practice for very serious threats to the safety of the country and to the safety of children. This will include the codes for stopping terrorists radicalising vulnerable users and stopping **child sexual exploitation and abuse**. The **Home Secretary** will agree these codes with the regulator.



> **Child sexual exploitation and abuse:** this is when a child is used for sex.
>
> **Home Secretary:** this is the person in charge of the Home Office. The job of the Home Office is to keep the public safe.

21. The regulator must work with the police and other organisations for codes of practice about:

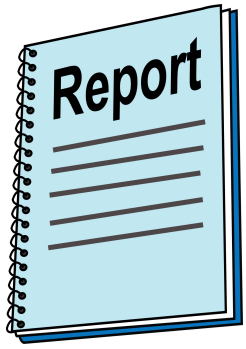
- Harm that is illegal for example **incitement of violence**

> **Incitement of violence:** this means information that pushes people to carry out violence.

- The sale of illegal goods and services such as weapons.

The regulator must work with the police and other organisations to make sure that the codes of practice keep up with what is happening.

22. Having a culture of **transparency**, trust and **accountability** will be an important part of the new regulatory framework. The regulator will have the power to ask for **transparency** reports from companies. These reports should give information about how much harmful information and material there is on their sites and what they are doing to deal with this.



> **Transparency:** this means that information is clear and open.
>
> **Accountability:** this means having a person or organisation that is responsible for something.

These reports will be put online by the regulator. This is so that users and parents can have all of the information they need to make a decision about how they use the internet. The regulator will also have powers to ask for extra information, such as:

- How algorithms work in choosing what information people see
- Making sure companies report on both harms that they know about and new harms that they see coming up.

23. The regulator will push companies to make it easier for researchers to access the information that they need. This is so that they can see how well those companies are doing in keeping people safe.

24. As part of the new duty of care, we will expect companies to have an easy way of making complaints too. This will be checked by the regulator. Companies will need to reply to users' complaints within a certain amount of time and take action.

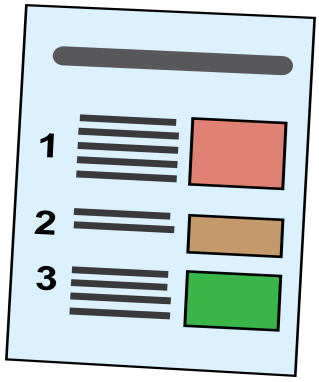
25. We also see how important an **independent review** is. This is to make sure that users have confidence that their worries are being treated fairly. We are **consulting** on different ways of doing this. One way of doing this is to allow some organisations to make '**super complaints'** to the regulator.

Independent Review: this is where a person or organisation looks at how well something is working. It is independent because the person or organisation doing the review is not connected to that organisation.

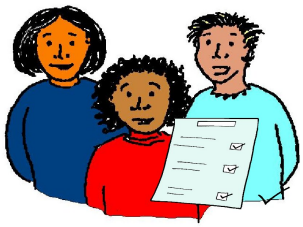
Consulting: here this means asking people and organisations for ideas.

Super complaint: this is when only certain organisations can make a complaint on behalf of people.

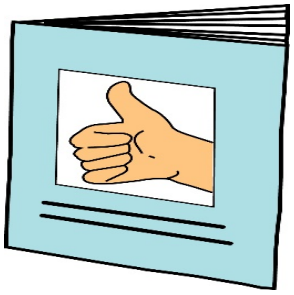
26. Before the new regulatory framework is put into place, we will keep on pushing companies to take steps to deal with online harms. To get companies started, this White Paper sets out what we expect of companies now. It has information about what we expect for different types of harm. The regulator should use this information in the future codes of practice.



27. For the most serious online crimes we will expect companies to show us what steps they will take to stop this information and illegal



behaviour from spreading. For example, for child sexual exploitation and abuse and terrorism we will write **interim codes of practice** later this year which will give a guide for what companies must do around these two areas.



Interim code of practice: this is a code of practice that is used before the final code of practice is ready.

The companies that come under the regulatory framework

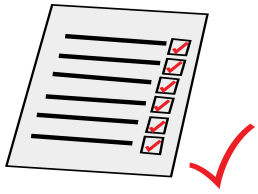
28. We think that the regulatory framework should cover companies that allow users to share or search for information written by users. Or companies that allow users to talk or communicate with each other online.

29. These services are offered by a lot of different companies of all sizes. These companies are made up of:

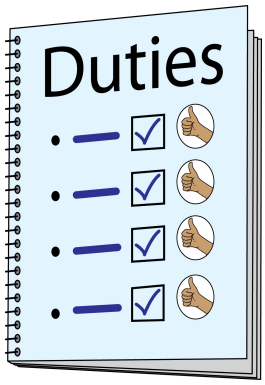
- Social media platforms.
- File hosting sites; this is a site where people can save and share files.
- Public discussion forums; this is a place online where people can talk about things.
- Messaging services.
- Search engines; this is a site that can be used to search for information.

30. The regulator will work in a way that first looks at which companies have the biggest risk of harm to users. This could be either because of how many users the platform is used by or because of issues with serious harms that they know about.

31. Every company that comes under this regulatory framework will need to meet their duty of care.



Companies will need to:



- Stop illegal information and activity.
- Send the information that is asked for by the regulator.
- Where needed, set up a way of dealing with complaints and **appeals** which is in line with the rules set out by the regulator.

Appeals: this is when a person or organisation does not agree with a decision and so they ask for the decision to be looked at again.

32. Privacy is very important, so private communications will not be checked for illegal information. We are now consulting on definitions of private communications and how these services could be made safer.

An independent regulator for online safety

33. An independent regulator will put in place the new regulatory framework, watch over it and make sure that companies keep to it. It will have enough **resources** and the right experts and skills to carry out its role.

> **Resources:** this means money, time and staff.

34. The regulator will deal with activity and information based on what is the biggest risk. This means the regulator will focus on where there is the most **evidence** of threat or harm, or where children or other vulnerable users are at risk. To support this, the regulator will work closely with UK Research and Innovation and other **partners.**

> **Evidence:** this means correct information.
>
> **Partners:** this means people and organisations that we work together with.

The regulator will set out what it expects companies to do to deal with harmful activity or information. What they expect the company to do will depend on:

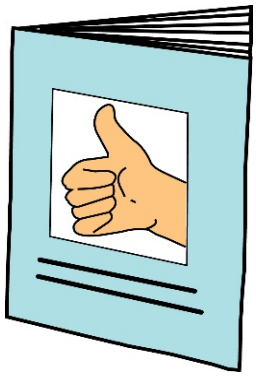
- What the harm is.
- The risk of the harm happening on the company's services.
- The resources and technology the company has to deal with harmful activity.

35. The regulator will have a duty by law to take account of **innovation**, and to protect users' rights online. They should take care not to interfere with people's privacy or freedom of expression. The regulator will not be responsible for deciding whether information online is true and correct.

Innovation: this means new ideas and ways of doing things.

36. The government is consulting on whether the regulator should be a new body or a body that already exists. In the future, the regulator will be paid for by online companies. The government is looking into ideas to pay for this work, such as companies paying fees or charges.

This could pay for:

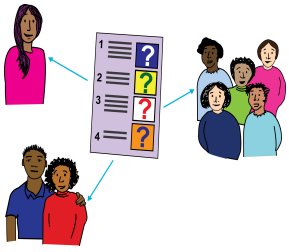


- Writing codes of practice.
- Making sure companies keep to their duty of care.
- Preparing transparency reports, these are reports about how clear and open companies are being around online harms
- Education and awareness activities carried out by the regulator.

Making sure the rules are followed

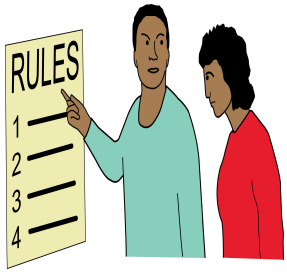
37. The regulator will have a number of powers to make sure the rules are followed. Such as the power to charge fines. This will make sure that all companies meet their duty of care.

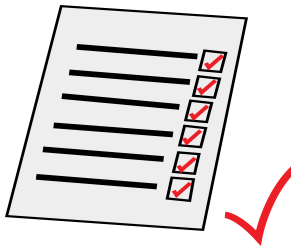
38. We are consulting on which powers the regulator should have. It is important to make sure that it is fair for UK companies and for those which are based in other countries.



39. We are also consulting on powers that would:

- Let the regulator stop the business activities of a company that does not keep to the rules.
- Make senior managers take responsibility for not meeting their duty of care.
- Give the regulator ways of stopping people from using services that do not keep to the rules.





40. The new regulatory framework will build on the responsibilities of online services, and keep them in line with the **European Union's E-Commerce Directive**.

> **European Union's E-Commerce Directive:** this is the set of European rules which organisations must keep to when doing business online. It sets out when businesses are responsible for information on their services and when they are not.

These rules now in place mean that companies are not responsible for any illegal information until:

- They know about it.
- And have not removed it quickly from their service.

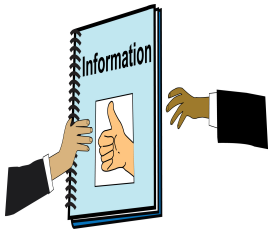
Technology as part of solving the problem

41. Companies should spend money on safety technologies to make it easier for users to stay safe online.

42. In November 2018, the Home Secretary ran a **hackathon** with five big technology companies. This was to design a way of dealing with online grooming.

> **Hackathon:** this is an event where a large number of people come together to do computer programming.

This solution will now be given for free to other companies. However, more of these efforts are needed, where we work together to come up with new ideas and ways of working.



43. The government and the regulator will work with leading industry organisations and other regulators to support new ideas and growth in this area. The government will work to push for more companies using safety technologies.

44. The government will also work with companies and the public to put together a **safety by design framework**. This will link up with laws and best ways of working around protecting people's information. It will make it easier for new companies and small businesses to make safety a part of their business from the very beginning. It will also make it easier when updating products or services.

> **Safety by design framework:** this means that safety will be thought about from the very beginning when online sites and services are being put together.

Giving users power

45. Users want to have the power to keep themselves and their children safe online. However, at the moment there isn't enough support in place, and many feel vulnerable online.

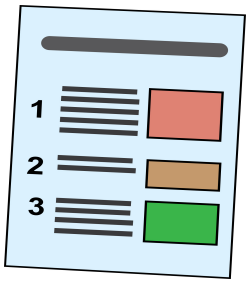
46. Companies are supporting a number of good pieces of work. However, there is not enough information about how much is being spent on this and how well it is working. The regulator will have access to this information.

47. The government will write a new **online media literacy** plan. This will be written in consultation with **stakeholders**. The big digital, broadcasting and news media organisations will be a part of this, along with education organisations, researchers and society in general.

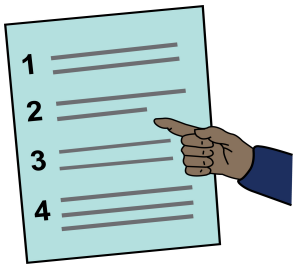
Online media literacy: this means how well a person can access, understand and use the internet and online services.

Stakeholders: this means people or organisations with an interest in this area.

This strategy will make sure there is a planned way of dealing with online media literacy, education and awareness for children, young people and adults.



Next steps

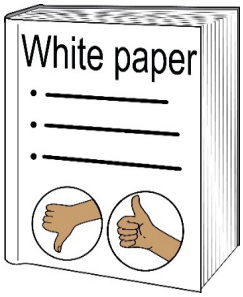


48. This White Paper sets out the government's planned way of working. This is a complicated and new area for **public policy**.

> **Public policy:** these are the actions, rules and laws decided by the Government.

For this reason, the White Paper also asks a number of questions about how the new regulatory framework should be planned. It also asks questions about other steps that could be taken that will not be a part of law. A full list of these questions is written below.

Consultation Questions



Please read the Easy Read Summary of the White Paper above and answer the questions below:

Question 1

The government has agreed to report on **transparency** each year. This means telling people about how open and clear businesses have been in sharing information with the government.

Other than what is written in the White Paper, should the Government do more to build a culture of **transparency**, trust and **accountability** across business? If you think that the government should do more, what do you think it should do?

Transparency: this means that information is clear and open.

Accountability: this means having a person or organisation that is responsible for something.

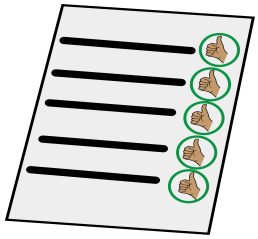
Question 2

Should some bodies or organisations be able to make 'super complaints' to the **regulator** in some situations?

Regulator: this is an organisation that checks that the rules around Online Harm are being kept to.

Question 2a

If your answer to question 2 is ‘yes’, in what situations should bodies or organisations be able to make ‘super complaints’?



Super complaint: this is when certain organisations can make a complaint on behalf of people.

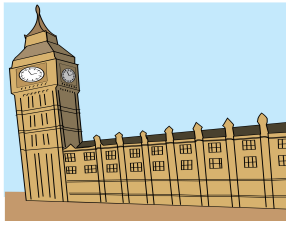
Question 3

In what other ways should users be able to tell the regulator about harmful information or activity online? In what way should users be able to tell the regulator that a company is not meeting its **duty of care**?

Duty of care: this is a duty in law. It means that an organisation must show how it takes care of the people that use its services.

Question 4

What role should parliament play in checking the work of the regulator? Should parliament be part of writing the **codes of practice**?



Code of practice: this is a guide about what people and organisations should do to keep to a law.

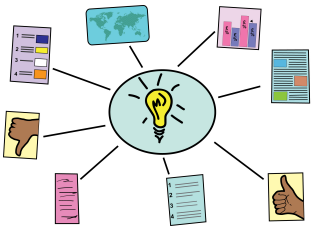
Question 5

Are you happy with our plans about which **online platforms and services** should come under the **regulatory framework**? You can look again at our plans in the section called 'the companies that come under the **regulatory framework'**, starting on paragraph 28 of the Easy Read White Paper summary.

Online platforms and services: this means sites or places online where you can buy and sell things or share information.

Regulatory framework: here, this means rules and laws written so that people and companies know what their rights and responsibilities are.

Question 6

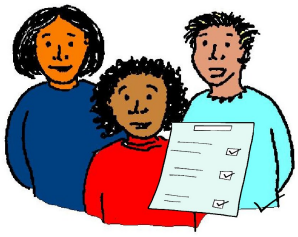


When writing a definition for what 'private communications' mean, what should we think about?

Question 7

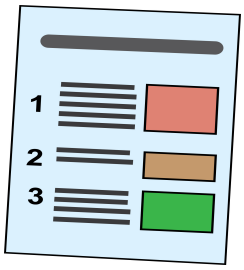
What ways of communicating online should be thought of as private and be a part of the regulatory framework?

Question 7a



What do you think we should ask private channels for communicating to do, so that we can deal with online harm?

Question 8
What steps could be taken to make sure that what the regulator does is aimed in the right way and is **proportionate**?



Proportionate: this means the right level of reaction to things that happen.

Question 9
What advice or support could the regulator give to businesses to help them meet the regulatory framework? Especially to new companies or small and medium sized companies?

Question 10
Should an online harms regulator be:

i. A new **public body**?
ii. A **public body** that already exists?

Public body: this is an organisation that runs a service for the public which is paid for by the government. However, it is not directly part of the government.

Question 10a

If you answered (ii), which body or bodies do you think it should be? This could be for example **Ofcom** or the **Information Commissioner's Office**.

Ofcom: this body is in charge of making sure competition is fair for communications companies.

Information Commissioners Office: this body pushes for the openness of public information and the protection of private information.

Question 11

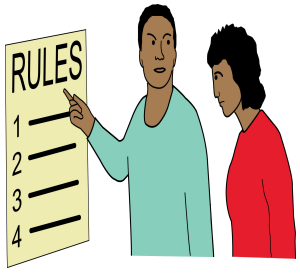
The regulator should be **cost neutral**. In what way should we decide which companies should pay and how much they should pay towards the costs of having a regulator?

Cost neutral: this means that the regulator will not cost anything to the taxpayer and will be paid for by the businesses that it is there to check.

Question 12

Should the regulator have the power to:

i. Stop business activities?
ii. Block websites or pages so that they cannot be seen?
iii. Be able to make senior managers in a company take responsibility for any online harm?



What other powers should the regulator have?

Question 13

Should the regulator have the power to make sure a company has a person in the UK who is responsible for keeping to online harms rules? This would be used when needed if the company is based outside of the UK or outside Europe.

Question 14

As well as a **judicial review**, should there be any way for a company to **appeal** a decision made by the regulator?

Judicial review: this is where a court can review a decision made or action taken by a public body.

Appeals: this is when a person or organisation does not agree with a decision and so they ask for the decision to be looked at again.

Question 14a

If your answer to Question 14 is 'yes', then in what cases should other ways of making an appeal be used?

Question 14b

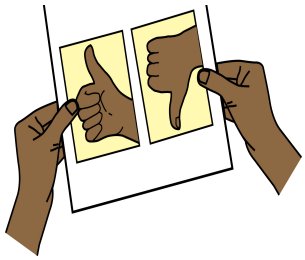
If your answer to Question 14 is 'yes', should the appeal be decided on in the same way as in a judicial review? In a judicial review it can only be decided whether the decision was legal or made in a legal way, it cannot decide what then happens.

Question 15

What are the biggest opportunities and barriers for:

i. **Innovation**?

ii. UK organisations using safety technology?



Innovation: this means new ideas and ways of doing things.

How should the government be a part of dealing with these barriers and opportunities?

Question 16

What are the most important areas where organisations need help building products that are **safe by design**?

Safe by design: this means that safety will be thought about from the very beginning when online sites and services are being planned.

Question 17

Should the government be doing more to help people stay safe online and keep their children safe online? If so, what should they be doing?

Question 18

What role should the regulator have around education and raising awareness of online safety issues?