Internet Safety

Submission of school pupils' views

to the Department for Digital, Culture, Media and Sport

on the Government's "Internet Safety Strategy" Green Paper

Summary

- **Views on internet safety are reported from 135 pupils aged 8 to 12 across 10 schools.**

- **Children's top five worries about going online or using social media or apps were being hacked or having personal information taken, being cyberbullied, people pretending to be other children or a friend to find out about you, advertised free offers that you end up having to pay for, and coming across offensive or rude things online.**

- **An overall worry was that "you don't know who's sitting behind the screen".**

- **The main things children saw as helping to keep them safe online, and on apps, games and social media, were help from their parents, being able to block people, reporting cyberbullies, age ratings on games, telling parents if they received 'mean messages', and antivirus software.**

- **Proposals to improve online safety included report and block buttons which are easier to find and use and which lead to seeing action taken, automatic scanning and deletion of harmful content, restricting the receipt of photos and messages on mobile phones to senders registered on that phone, more safety education, stronger penalties for harmful behaviour online, including reporting to the police, laws to remove harmful material from websites and harmful games, being able to refer an offensive player of an online game to the game's supplier for the player to be suspended, and means to provide support to victims of cyberbullying – such as children being able to write a stock of supportive poems to be sent to victims.**

- **There needs to be continued work on protecting against hacking and viruses, improved privacy and confidentiality, use of age restrictions, parental supervision of children online, on ensuring that the 'internet of things' (such as things around the house connected to the internet, and driverless cars) do not bring hacking risks, and on frequent changing of passwords.**

- **85% thought they knew well how to keep themselves safe online, 15% were not sure how well they really knew how to stay safe.**

- **The top three sources of children's information on how to keep themselves safe on the internet were, in order, teachers, parents or carers, and relatives (not counting brothers or sisters). Just over a third had got internet safety information from brothers or sisters. Just under one in five had got internet safety information from friends.**

- **The children supported the Government's proposal for a Social Media Levy by 47% to 20% (with 33% in the middle). Their top three priorities for spending from a Levy were developing safer technology, supporting charities working to keep children safe online, and more resources for schools to teach internet safety. Their bottom three priorities were general awareness campaigns, resources for parents and carers to teach their children internet safety, and spending on children teaching internet safety to other children.**

- **The children's top three priorities to go into a Code of Practice for social media organisations were keeping privacy, how to find and stop people doing things that aren't allowed, and reporting bullying or things that are harmful. They proposed that the Code should include making report buttons effective and easy to find and use.**

- **Children voted in favour of the Green Paper proposal to make all schools teach internet safety as part of their teaching about relationships, by 72 to 27.**

- **Children wished to add teaching at all schools about recovering from being cyberbullied or a victim of internet harm.**

- **56 children gave views on the Government proposals to develop 'peer to peer' spreading of internet safety information by children to other children. There was overall support, with 56 views in favour (mainly agreeing that children would listen well to information from other children, and that it was a good way of spreading information), and 27 against (mainly concerned that peer to peer teaching could easily spread incorrect information, either deliberately or accidentally, and that there were better ways of teaching children correct safety information).**

Introduction

1. This report is a formal submission to the Department for Digital, Culture, Media and Sport on the *Internet Safety Strategy* Green Paper.

2. The report is from Pupils 2 Parliament, a project to enable school pupils to consider and feed in their views to parliamentary, national government and national body public consultations and inquiries. The project has been approved by the Clerks of both Houses of Parliament to use the term 'Parliament' in its title.

3. Pupils 2 Parliament aims to bring the particular viewpoint of children and young people to those conducting inquiries and consultations - plus the uniquely fresh and often challenging analysis that children and young people bring to decisions and policies.

4. The project also gives school pupils the chance to learn about and consider key issues and decisions being made by parliament, national government and public bodies, and genuinely to participate in democracy by feeding their views into real national decisionmaking.

5. Pupils' views are independently gathered through discussions with groups of pupils led by someone from Pupils 2 Parliament, with a member of school staff taking notes of the pupils' views. We use information from the relevant consultation or inquiry document to explain the issues. We specialise in putting the issues and questions even-handedly, without leading pupils in any way or suggesting any responses. All views come spontaneously from pupils, with no adult prompt on what they might say.

6. The information we gave to pupils about this inquiry came from the Green Paper itself. We explained that we wished to hear their views about safety online, when using mobile phones, on social media and when using different sorts of apps. We said we knew that many would already be using these, and many would not be using them yet at their age, but that they probably would be in the future and so their views were equally important. Our questions to the children were based on the issues and proposals in the Green Paper, with some questions taken from the Government's survey document for adults.

7. This report contains all pupil views given, without selection, comment or addition. The views reported are entirely pupils' own views, and nothing but pupils' views.

8. Views in the report came from 135 school pupils aged 8 to 12, in 5 pupil focus groups involving 10 schools. These groups were of pupils at Moor Park Preparatory School, Ludlow; Peters Hill Primary School, Brierley Hill; Howley Grange Primary School, Halesowen; and Presteigne Primary School, Powys; together with a group from the Stourbridge Partnership schools with representative pupils from Quarry Bank Primary School, Brierley Hill; Hob Green Primary School, Stourbridge; Pedmore CofE Primary School, Stourbridge; Ridgewood High School, Stourbridge; Amblecote Primary School, Stourbridge; and Rufford Primary School, Stourbridge.

9. This report represents the vital perspectives of children on internet safety, and I hope that their views will provide a valuable input to the development of the proposals in the Green Paper - separately from the views of adults which will have been sent in through the online survey for adults.

What worries children most about going online or using apps?

10. We asked all children in all groups what worried them most about using the internet, mobile phones, social media, apps and online games.

11. By far the two most common worries were someone hacking into your account or finding private information about you (this came from 15 children), and being cyberbullied (this came from 11 children). Cyberbullying included being sent unpleasant or "mean messages", or having photos you had sent to someone then sent on to lots of other people.

12. These were followed by three different but equal worries. One was someone pretending to be your friend or someone else to get information about you - "someone pretending to be someone else and you tell them about yourself", "someone tricks you into thinking they're your friend", "people might have a nice picture but might not look like that in real life". Another was false advertising , which offered you something (such as a game) for free, but still ended up charging you - "free offers that aren't free". You could find that clicking onto something you thought didn't cost anything ended up in a bill being sent to your parents. The third worry was coming across offensive things online – "finding things that personally offend me", "if you search pictures then the wrong sort of pictures might come up", "seeing rude things".

13. There were other worries about people tricking you to get private information about you, or you accidentally giving away personal information about yourself. These included being asked for your personal details when registering for something, being hacked from someone's phone, fake websites, downloading a false app that then says it has stolen information about you, getting your password hacked or stolen or getting tricked into giving your username or password online. These things could be to take something from you, such as emails pretending to be from a bank and persuading you to send your money to someone else, or someone finding out your bank details. They could also be to send unpleasant messages to you, or to send unpleasant messages to other people that looked as if they came from you. They could be to blackmail you, or to send you threats.

14. Sometimes sites and apps tried to trick you into giving away your personal details, but often they are designed so that you have to give personal details before you can register or buy something on them.

15. There were also worries that someone you don't know could be learning things about you, in order to harm you. You could be asked where you live, or people online could work out where you live in order to find you. Such worries also included strangers talking to you online, and people asking you questions on social media in order to find you. There was the worry that people you don't know might ask you online to meet up with them in real life. One child said a worry was getting stalked online. Another said they were worried about an adult pretending to be a child in order to kidnap them.

16. Children had a number of other worries about not knowing who you might be in contact with, or be contacted by, online. Someone you didn't know might join your online game; when you send an email you might not be sure whether you are actually emailing the person you intend to; you might get messages or calls you don't know about or from people you don't know; you often got friend requests from people you don't know; and there were the risks of answering texts from people you didn't know.

17. One worry about talking to strangers online was not to do with any risks from those strangers, but the worry that you could get into trouble if you had been talking to someone you didn't know. People could get cross with you if they found out you hadn't done all the right things to keep yourself safe online.

18. Another particular worry was not knowing how to report unpleasant or harmful things you came across online. This could be not knowing where the report button was, and getting asked lots of questions (some of the sort you were told not to answer online) as a result of pressing the report button, which could lead you to give up on reporting something. You also didn't really know what happens when you press a report button. Many children suspected that not much would happen.

19. Some other worries were not knowing how to get rid of an advert or photo that appears on your screen, being asked for personal details or even a photo of yourself when you log into a game, someone stealing something someone else had put online and claiming it is theirs, people being racist or swearing online, getting a virus on your

machine from a link you follow, getting "spammed", and accidentally clicking onto something you shouldn't.

20.   A general worry of many was put in these words by one pupil: "you don't know who's sitting behind the screen".

21.   Another was about the lack of privacy online: "I hate the idea of people around the world being able to see you on social media", and the risk of having pictures you have sent someone getting spread to other people – "pictures without permission".

What do children think helps to keep them safe online or when using apps?

22.   We then asked children what they thought kept them safe online now. We have listed all the answers they gave.

23.   The two most common answers were:

- Parents
- Blocking people to stop them sending you anything else unpleasant.

24.   The next four most common answers were:

- Reporting cyberbullies
- Age ratings on games, and not buying or playing games rated older than you are
- Telling parents if you receive mean messages
- Antivirus software.

25.   After these, there came:

- Only visiting known and trusted websites
- That the creators of games and apps may be watching to see how their creations are doing
- Private areas on sites
- Never telling anyone your private information
- Using privacy settings
- Never giving your personal information.

26.   Two children gave us important mottoes to keep safe: "Just be careful", and "think before you do something".

27.   The other answers, which each came from one or two children only, were:

- Not answering a message unless you know the person it's from

- Knowing where the report button is
- If something pops up on your screen and you don't know what it is, telling an adult
- The CEOP button
- Always having an adult with you when you're online
- Not telling anyone your passwords or usernames
- Not 'adding' anyone unless you know them
- Passwords
- Making sure your passwords have at least 8 characters and symbols
- Changing all your passwords every six months
- Not going on something without permission
- Not going on sites or apps where you can speak to people, without your parent's permission
- Read what personal information you would be asked to give, before deciding to download anything
- Getting a parent's permission before downloading an app
- Using hashtags which prevent people from being mean to you online
- If you make a video, blocking people to stop them copying and changing it
- Making your parents a 'friend' on sites and apps so they can see what you're up to
- Always knowing how to contact your parents in case you need to
- Not signing on to sites as a 'guest'
- Not answering your phone if you don't recognise the person or number
- Not talking online to someone you don't know
- Not going on something an adult tells you not to – they tell you for your safety
- Not making friends with someone online unless you've met them in person
- Not going on YouTube channels where people have copied a popular channel
- Don't give personal advice online
- Having two or three steps to buy or confirm something
- Having to choose which way you are going to pay, making it difficult to buy something accidentally
- Having to use 4 different passwords to get into your password store
- Firewalls (though these are strong and give you warnings, they don't stop everything they should)
- Fingerprint recognition on phones
- Laws
- Childline
- Never giving your bank account details
- Teachers
- Scans
- Reporting things online
- Blocking people
- Only using trusted search engines (such as Safesearch, though this doesn't always work)
- Flagging people you know to be rude
- Keeping friend requests only to people you already know
- Keeping away from apps with advertising
- Not giving names or dates of birth of brothers, sisters or other family members

- Telling and asking friends how to report or block things online.

What more do children propose to keep them safer online or on a mobile phone?

28. After asking about staying safe now, we asked all our pupils whether they had any proposals for future work or anything new to keep us safer online in the future. Here is the full list of their proposals:

- Make reports of continuing unacceptable behaviour online to the police
- Work on getting rid of fake accounts
- Make servers more private
- Work to stop hacking
- Requiring retyping of all passwords every week
- Require a password before going onto any site offering to sell things (it is now possible to go onto selling sites and apps without entering any password)
- All apps should have age ratings and require parental permission to download
- Require any child under 8, or any older child or adult without full understanding, to be accompanied by a parent or other responsible person before they can go online
- Develop automatic scanning of emails and messages to delete bad content
- Make mobile phone controls which only allow anything to be received from people you've set as approved to send you things
- Be able to delete any email or message you send within a period of time before it is transmitted, in case it is a mistake or you have second thoughts about it
- Make it impossible to buy anything online without saying 'yes' extra times – to prevent accidentally buying things
- Make sure children cannot use things like Instagram until they are the right age
- Make it easy to blur out parts of pictures you send on social media, to cover up any personal details on documents or address details
- Make it harder to access games containing inappropriate language – harder than just using a password
- Work to reduce hacking through the internet of things, such as internet connected things at home or driverless cars
- Have stronger penalties for bullying anyone online
- Make it easier to block unpleasant messages
- More work to avoid viruses
- Make it compulsory to delete bad stuff from websites
- More telling of people what to do and what not to do online to keep themselves safe
- Easier use of # to keep information confidential
- Making it law that a game could be removed if being used harmfully
- Systems to make sure your parents can see what you have been playing online and what texts you have received
- A system on games where you can forward unpleasant comments or content to the game's creators, requiring them to suspend offending players from playing that game if they agree it was inappropriate.

29.   Many wanted 'report' and 'block' buttons on sites and apps to be improved. Users should be told where the report and block buttons are. Report and block buttons should be made "bigger and brighter", and made easier to find – putting them in the same place on all sites, and showing you where they are whenever you open any game. The buttons should be easier and quicker to use – fast to "send wherever it goes", and not asking you so many questions before they do anything that you give up on them. Not all thought anything happens when you press a report or block button, so it was important that something actually gets done whenever a report or block button is pressed.

30.   There was some disagreement over apps and games asking your age or date of birth to try to make sure you didn't go somewhere that was age-rated as older than you are. Some thought that though people may not be truthful, it was better to ask your age or date of birth than not to, in order to check this. Others thought you should never have to supply personal information such as your age or date of birth online. Some said that only the major app stores should be allowed to ask you for your age to check against the age-rating of anything you wanted to download, but not individual apps, sites or games.

31.   One proposal made was that if you see anyone being mean to someone on a game, you should be able to send a message of help and support to the person who has been mean to.

32.   Many thought what was needed was to do better at things that already help to keep children safe online. These included trying to avoid viruses, calling parents if you find something unpleasant online, "doing a lot of blocking", not replying to people you don't know, never using your real name as a username, not telling people your date of birth online, and deleting an app if someone is hacking you. One pupil wondered whether they should "hack the hackers back".

How well do children know about ways of keeping safe online or on a mobile phone?

33.   We asked all 135 children to tell us how well they thought they knew about ways of keeping themselves safe online, on mobile phones, and when using apps and social media.

34.   None of the children thought they were unaware of ways of keeping themselves safe. None answered that they knew 'not much' or 'not at all' about keeping safe.

35.   Most children (62 percent) said they knew 'pretty well' about ways of keeping safe on. Another 23 percent said they knew 'very well' about ways of keeping themselves safe. This makes 85 percent who thought they knew well how to keep themselves safe online.

36.   However, 15 percent of the children answered that they were not sure how well they really knew how to keep themselves safe.

Where children get information about keeping safe online or on a mobile phone

37.　　We asked children where they had got information from about how to stay safe on the internet, on mobile phones, social media or other apps. We asked how many had got information from each of a list of different sources, and then asked them to tell us of anywhere else they had got information from.

38.　　Here is the list of the people and places children had got information from about staying safe online, with the most usual source of information at the top. The numbers are the percentages of the 135 children who had got their information from that source:

- Teachers (79%)
- Parents or carers (68%)
- Other relatives (not including brothers or sisters) (60%)
- From the internet itself (44%)
- Television (43%)
- Brothers or sisters (including half siblings and step siblings) (36%)
- Leaflets (31%)
- Friends (19%).

39.　　Almost a quarter of the children (24%) had got information about keeping themselves safe from other people or places. Three children had got information from talks by the police, three from what they had read in books, and three from visitors (including students) coming to the school to tell pupils about internet safety. Another three said they had worked out how to stay safe for themselves.

40.　　Two children had got safety information from safety messages on social media itself, two from YouTube, and two from signs or posters on walls. Two had been given safety information by their childminders.

41.　　Sources of information which had provided safety information for one child each were: an app, an online trailer, a social media 'censor', the manufacturers of their electronic equipment, a mobile phone shop, the terms and conditions for a game or app, adverts for online games, their dentist, information on their iPad, advertisements, and an internet safety charity.

42.　　One child told us they had learned how to keep themselves safe as a result of their own experience of something unpleasant happening to them online.

43.　　Overall therefore, the sources of information on internet safety which had each given information to over half the children were, in order, teachers, parents or carers, and relatives other than brothers and sisters. Just under one in five children had got internet safety information from their friends.

Children's views and vote on the proposed Social Media Levy

44.   The Green Paper proposes that social media companies and organisations should be asked to pay money into a national fund, which would then be used to pay for making the internet and social media safer. This would be called the 'Social Media Levy'. If not enough money was paid in by enough companies and organisations, the law could then make them pay money into the fund.

45.   The Government's survey for adults asks adults to say whether how strongly they are for or against the idea of the Social Media Levy. We asked the same question of all the children.

46.   Overall the children agreed with the Government proposal to set up a Social Media Levy. Almost half the children (47%) voted for the proposal. 32% agreed with it, and 15% voted that they strongly agreed with it.

47.   One in five (20%) voted against the proposal. 11% disagreed with it, and 9% strongly disagreed with it.

48.   There was though a lot of uncertainty about the proposal among the children. One in three (33%) said they neither agreed nor disagreed with it.

49.   One view was that if money can be gathered to improve things for people generally, homelessness was more important than internet safety for it to be spent on. Another was that any money available would be better spent on medicines and helping disabled people.

50.   We asked three of our five children's groups what should be the main things the money in a Social Media Levy should be spent on. We gave them a list chosen from the list in the Government's survey for adults.

51.   Over half the children wanted much of the money spent on each of these from the list (in order, with the most wanted first):

- Developing new technology to keep children safer online
- Charities working to keep children safe online
- Resources for schools and clubs to teach children how to stay safe online
- Code clubs to teach children how to write programmes for computers and to stay safe online
- An online Safety Advice Centre
- Resources for professionals (other than teachers) working with children to teach online safety.

52.   These ideas for funding from a Social Media Levy were each chosen by fewer than half the children. Again the list is in order, with those that got the most votes first:

- Campaigns to make people generally more aware of online safety
- Resources for parents and carers to teach children how to stay safe online
- Children learning from other children about safety online.

53.   Some children made their own proposals for spending from the Social Media Levy. These were:

- Stopping rude advertisements
- Making new games based around e-safety
- Making more websites giving information about e-safety
- Developing an app that alerts you if someone is trying to hack you, so you can switch off
- E-safety clubs
- A lock stopping you coming across rude things when you are searching online
- Teaching homeless people to stay safe online
- Working on ways to stop viruses from spreading.

54.   One proposal was that half the money in the Social Media Levy should be spent on what people thought was needed now, but half should be put aside to spend when people could see what was happening online in the future.

What children want to go into the Code of Practice for social media companies

55.   We asked the children what they wanted to see the Government put in its Code of Practice for social media organisations. We asked two of our children's groups which they most wanted to see in the Code, from the list of Government proposals.

56.   The things they wanted to see in the Code of Practice (in order, with the most wanted first), were:

- Rules about keeping people's privacy
- How to find and stop people doing things that aren't allowed on apps and sites
- Better ways to report bullying, harmful things, or things you don't think should be allowed you find on apps and sites
- The rule that when something is reported as bullying or harmful, the people running the app or site should *either* take them down, *or* explain why not
- What *should* be allowed on apps and sites.

57.   Children made an additional proposal for the Code of Practice. This was that all providers of sites, apps and games, should make report buttons easy to see and find, and always in the same place for all of them.

Making schools teach internet safety as part of teaching about relationships

58.   The Government proposes that, by law, schools should all teach their pupils internet safety as part of their teaching about relationships between people.

59.   We asked children to vote on this proposal to make internet safety part of teaching about relationships between people that schools must legally give. 116 children voted. The vote was strongly in favour of the proposal, by 72 votes for and 27 against. 17 said they didn't know whether to support or oppose the proposal.

60.   Some children proposed what teaching should happen in schools. Some thought that police should come into schools to teach e-safety. Others recommended that all teachers, including those in high schools, should teach e-safety to all their pupils.

61.   A strong recommendation was made by some children, in different discussion groups, that schools should not only teach how to keep yourself safe online, but also how to survive and get out of a bullying situation once they had got into it. There should be "lessons about how to recover from cyberbullying".

62.   One child proposed that children should be given time to write poems, which could then be sent to people who have been the victims of cyberbullying, to make them feel supported.

The children's view of peer to peer training for children

63.   One of the Government's key proposals in the Green Paper is that 'peer to peer' training should be more developed in schools. This is where some children are given some internet safety training to share in different ways with other children at school. The Government believes that children will often learn some things better from other children than from adults.

64.   We wanted to find out what the children themselves thought about this. A few had already taken part in peer to peer training, either about internet safety or by being 'ambassadors' to other children for other things.

65.   We asked those who felt able to give a view on peer to peer training, to say whether they were for or against it, and to give reasons for their position. 56 children gave their views. 41 gave reasons for peer to peer tuition, and 15 gave reasons against it.

66.   Children's reasons in favour of peer to peer training were their own positive experience of doing it already at their schools, and that children will learn well from other children ("children will listen to children instead of grown ups", "children find other children more interesting"). It is good for children's education to share knowledge, both for those giving the information and for those learning it. "Children would teach in a different way to adults". Children are likely to know more about the internet and social media than adults do, and children who have learned something from other children are more likely to pass it on themselves. Peer to peer training should do well in raising awareness of internet safety among children, and it also allows children to find out about safety and what they should and shouldn't do without having to go to an adult. Children sharing information about internet safety between

themselves may also help children not to feel so sad about cyberbullying, and to ask other children how to stop it.

67.   Those who gave reasons against peer to peer training said that children may get things wrong, they may get bossy with other children, they may "make stuff up" and pass on their own ideas and things that aren't true, they may change words and accidentally get things wrong, and they may get distracted from what they are supposed to be passing on. Children may not know enough about safety, even after they have been told about it, to give the right advice, and teachers may well actually know more about staying safe than children do. Some children don't understand things the way other children put them, and children may not take other children seriously enough. If children tell others lies or things that are wrong, that is likely to get spread around more children. There was a worry that "some kids can be mean", and those passing things to others could be tricking them.

68.   There was also a view that the Government and schools "shouldn't have to go through all that" – it was ok for teachers and expert visitors to teach children about internet safety. There could also be better and easier ways of training than using children to teach children, like developing online apps and quizzes to teach internet safety.

---

69.   I am grateful to the Heads and staff of the nine schools for letting me carry out these discussions with their pupils, to the members of staff who took notes of the pupils' votes and views, and above all to the pupils themselves who gave their fresh thinking, views and ideas for this report.

Dr Roger Morgan OBE
Pupils 2 Parliament

5th December 2017