Safe Online in 2017

A ‘State of the Capital’ Report from

LGfL DigiSafe

Powered by data collected from pupils
from January to August 2017
from the CyberPass online-safety diagnostic tool
(August Update)

LGfL DigiSafe

LONDON GRID FOR LEARNING

TRUSTnet

Background information

Who or what is LGfL DigiSafe?

The London Grid for Learning is an educational charity which serves schools in London as LGfL and across the UK as TRUSTnet, providing schoolsafe fibre broadband, technical services, online learning and centres of excellence in SEND and online safety & safeguarding.

LGfL DigiSafe is the new Centre of Excellence in online-safety and safeguarding for LGfL and TRUSTnet, designed for one of the eight core aims of the LGfL Trust: 'Keeping Children Safe', which guides and permeates all that we do.

Find out more about LGfL at lgfl.net, about TRUSTnet at www.trustnet.pro, and about our online-safety and safeguarding work at digisafe.lgfl.net.

What is CyberPass?

CyberPass is an award-winning trackable online-safety diagnostic tool which allows teachers to take a snapshot of their pupils' abilities, informing targeted and effective classroom interventions. Pupils take quizzes to reveal strengths and weaknesses across eight core online-safety themes, which in turn are divided into 85 competencies; teachers see class and individual data at a glance from a handy teacher dashboard.

To find out more about CyberPass, visit cpinfo.lgfl.net

What is this report?

CyberPass generates hundreds of thousands of lines of data every term, and this new regular report is intended to share this data with all interested stakeholders, highlighting the state of the London schoolchildren's online-safety prowess (or otherwise), including strengths, weaknesses and anomalies, and trend analysis over time.

Who is it for?

The report will be of interest to teachers, senior leaders, parents and governors alike as they consider online-safety and broader safeguarding provision at their schools.

What about my school?

If you are an LGfL school using CyberPass, you may want to download all the data for your school to do a similar analysis for pupils in your context. Any member of staff who has been assigned the 'CyberPass Administrator' flag can do this from their dashboard (visit cpinfo.lgfl.net for FAQs and 'how-to' documents).

Executive Summary

This report offers an analysis of the data collected from two terms' use of the CyberPass online-safety diagnostic tool by London schools in the Spring and Summer school terms of 2017 (1 January to 31 July).

Over half a million questions were answered: encouragingly, 74% of which correctly. The data in this report reveals an interesting snapshot of pupils who are seemingly well acquainted with education messages about dealing with friends and what to share online, but raises the question of why it is not always translated into practice.

The report also shows that young people still struggle to identify the basic hallmarks of a secure website and that online money matters and safe searching are worrying areas of weakness which schools, parents and providers of online-safety resources needs to be aware of and to address, especially as ransomware, phishing and other malware attacks proliferate and succeed against individuals and even national infrastructure.

Read on to find out more (key figures are overleaf). Alternatively:

o More information about the CyberPass resource:	cpinfo.lgfl.net
o Online-safety resources for parents, teachers and pupils at	osresources.lgfl.net
o Subscribe to our blog at	safeblog.lgfl.net
o Sign up for a fortnightly newsletter for DSLs and OS leads	safenews.lgfl.net
o Follow us on Twitter	@LGfLDigiSafe
o Like us on Facebook	facebook.com/LGfLDigiSafe

Key figures for this report

Dates

Most schools engage with CyberPass at one specific time of year. This report is based on data generated from those schools which deployed the tool during the Spring and Summer terms of 2017, that is between 1 January and 3 April 2017. Autumn term data (September – December 2016) was not included due to mathematical changes in the back end which would distort the overall year's view when viewed as one.

Who and how many?

As you can see from the following figures, the scale and scope of users and questions taken provide a highly valuable and statistically relevant data set.

During the entire 2017/2018 academic year, 12,728 pupils drawn from 642 schools answered 951,253 online-safety questions. During the period covered by this report:

7,866 pupils drawn from

496 schools answered

527,619 questions on online-safety issues, and

74% were correct

Baseline figure

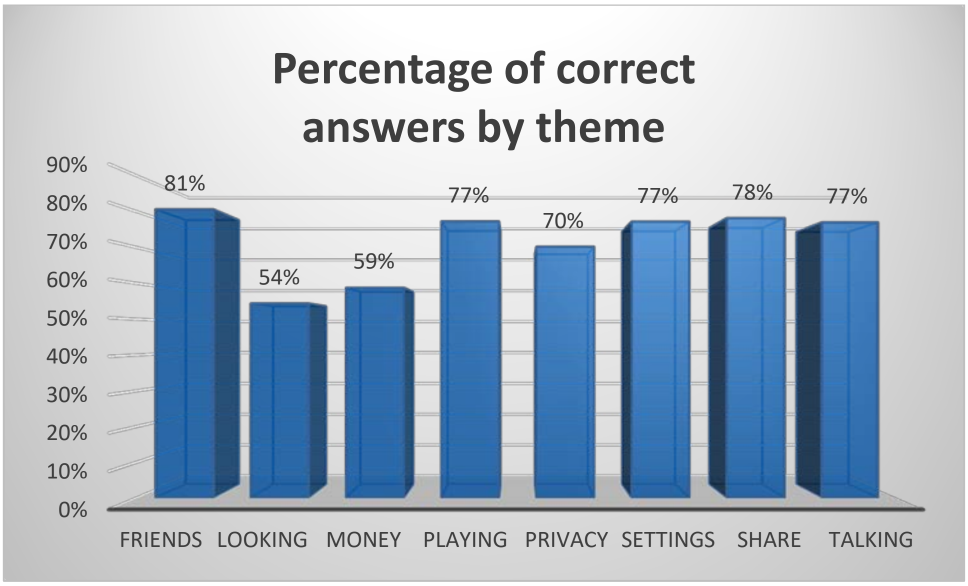
Of all the over 500,000 quiz questions asked during this period, London's pupils answered 74% correctly. Whilst this is at face value an encouraging number, it cannot be viewed without considering many other factors and drilling further into the data. The following pages help break down the figures and give a high-level analysis of some of the issues raised.

Changes between Spring and Summer terms

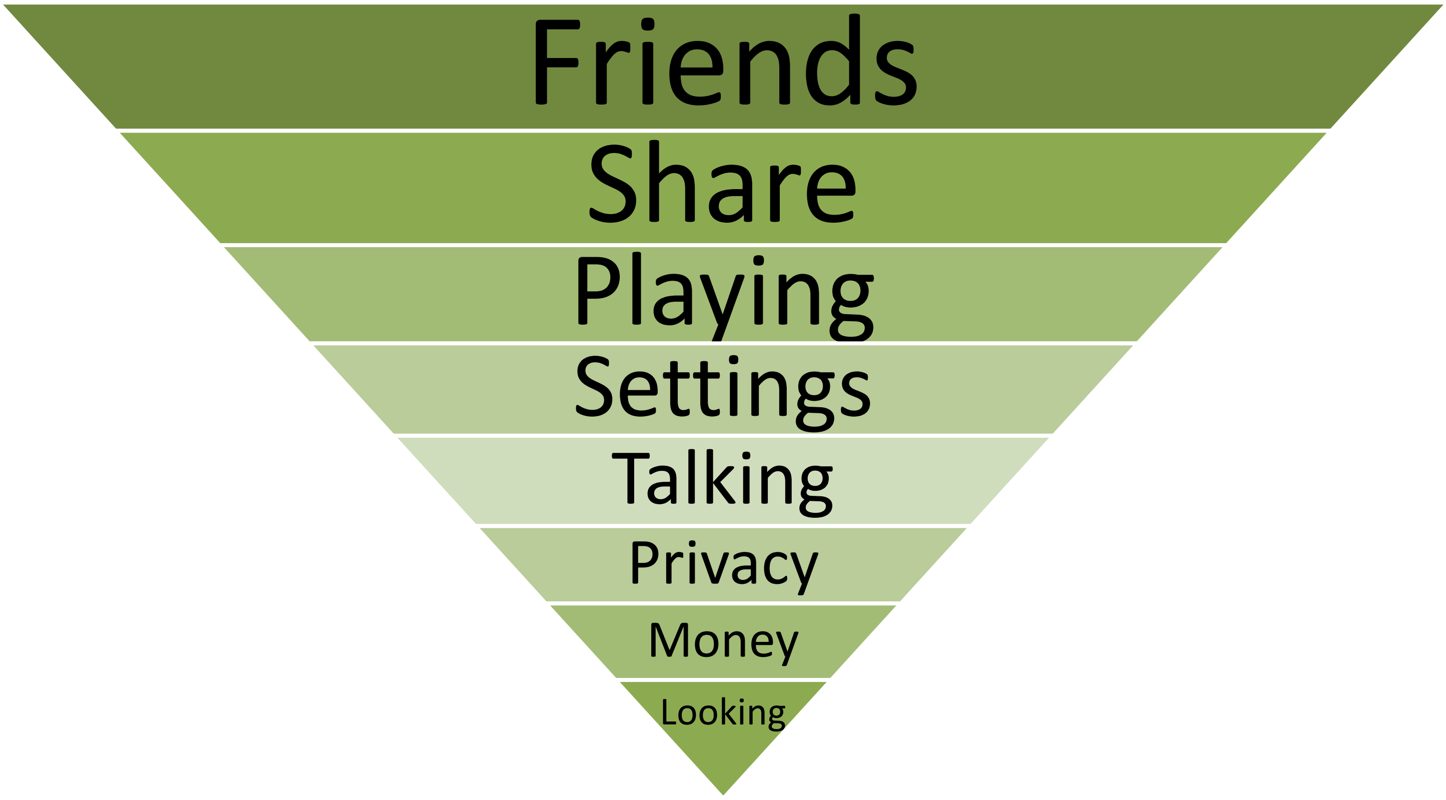
There are no significant changes between the two terms, which are in any case too short to identify trends. The 74% success rate does not change when broken down by term; figures for the eight themes do not change by more than 1 percentage point, and the order of themes in terms of strongest and weakest do not change between Spring and Summer. There were only two instances where one of the themes' strongest and weakest sub-competencies (of which there are 85) changed, and of all sub-competency results, no more than a two percentage point change was noted between the terms. Accordingly, the two terms are treated as one reporting period – in the three instances where the strongest and weakest competencies within a theme have changed over that period, this is highlighted in the relevant section of the report.

Theme overview*

Relative areas of strength and weakness



Ranking of relative strength (strongest theme first)


Friends

Share

Playing

Settings

Talking

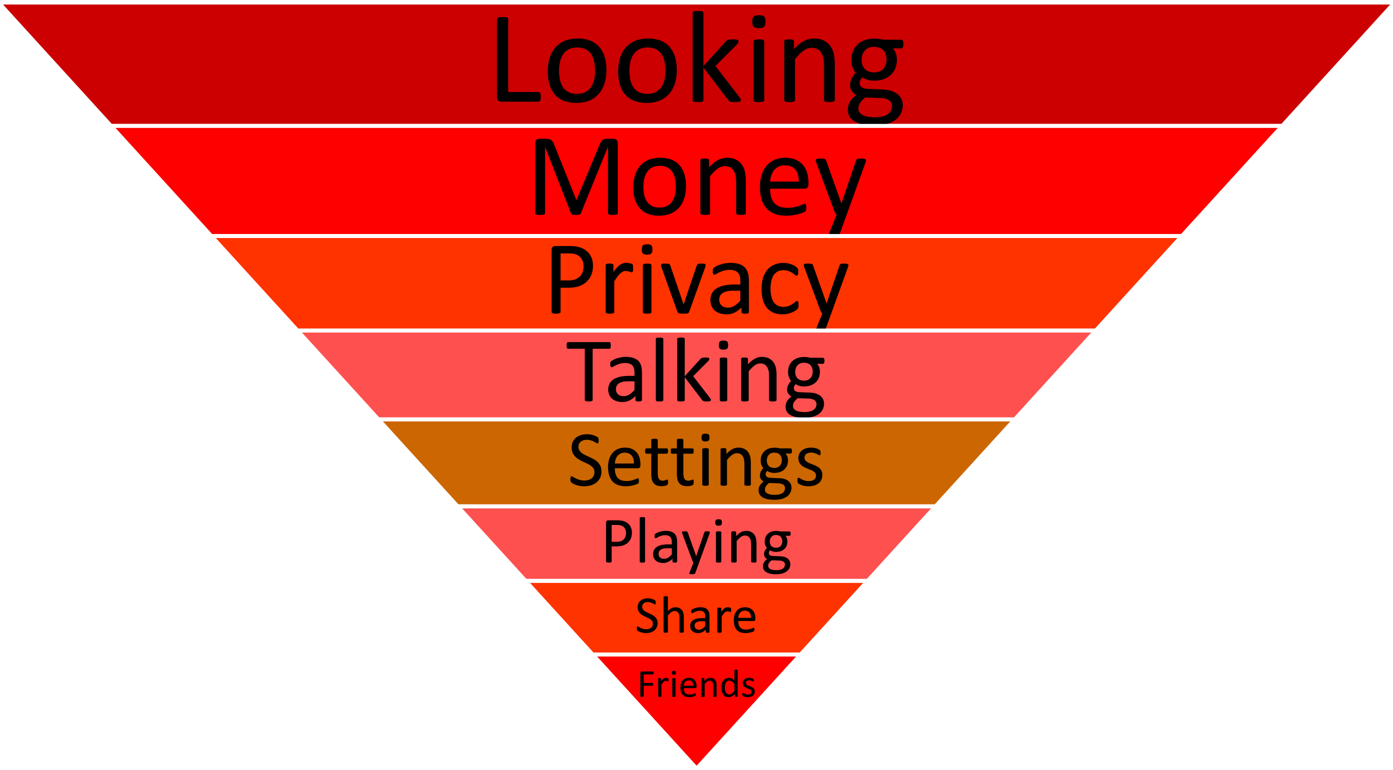
Privacy

Money

Looking

** The full charts with all raw figures are included as Appendix 1 to this report*

Ranking of relative strength (weakest theme first)



Before analysing these overview findings (the most obvious surprise being an apparent discrepancy between this evidence that ‘Friends’ is a strength, in the context of anecdotal and empirical studies to the contrary), let us first break down each theme into its constituent competencies.

Competencies by theme* (two weakest / strongest competencies)

Friends (strongest area – 81%)

Knowledge that all is not what it appears online and that sometimes people can use the web to make contact for "bad" reasons.	65%
Management of privacy settings and friending.	70%
Matching of behaviour to situations.	91%
Recognition of inappropriate behaviour and strategies to mitigate and manage the social ramifications of reporting and "unfriending".	91%

If the average online-safety lead in a school were asked to identify an area of strength in the online-safety competence of young people, they would be unlikely to identify dealing with friends online as a strength, albeit against a background of young people living out their friendships online (and therefore developing a deep well of experience to draw from).

This finding perhaps shows us that young people are hearing and understanding messages about how to treat friends online but then choosing not to apply them in practice or not being able to as they are not relevant or useful. This area requires further study but providers of online-safety resources should bear this in mind.

In my school

Why not ask the people who know? Take some time with pupils to ask them what they think of the messages we give them and if they are helpful/relevant or not? What messages do they think we should share about friends and bullying? Let us know what you find out!

Resource tip

Check out the list of resources we have curated for you at bullying.lgfl.net – one we love is the PSHE Toolkit on CyberBullying from Childnet.

* See Appendix 1 to view all other competencies (only top and bottom two are presented here)

Share (2nd strongest area – 78%)

Ability to make a 'mash-up' with appropriate permissions.	71%
Identification of plagiarism and its inappropriateness.	71%
Understanding that the use of Snapchat or Skype does not preclude images from being stored on the Internet.	85%
Identification of the ramifications of breaking the rules.	89%

This area is fairly broad, covering issues such as copyright and also sexting, but also seems surprising as an area of strength given practice on the ground. Adults are frequently caught out by all these issues, and it may be the case that we are demonstrating different message to the ones we are teaching.

In my school

As with the previous topic, start a discussion with pupils on whether our messaging is inadequate or patronising, or are adults simply missing the point? Also ask if they see adults being careful about copyright and intellectual property online, or indeed about sharing revealing pictures? Is there a perceived hypocrisy (beware you don't get told by your class that they have seen your holiday snaps on Facebook)?

Resource tip

Various filters on LGfL DigiSafe's online-safety resources portal (osresources.lgfl.net) cover this area, such as downloading, safe surfing, online privacy and sexting. Why not check out the 'Copyright Uncovered' lesson from Digizen or 'So You Got Naked Online' from SWGfL for a different approach to sexting?

Playing (77%)

Understanding that users of social media sites have a responsibility to behave in an acceptable manner.	48%
Knowledge that all data on the Internet is permanent.	58%
Risk minimisation strategies for online gaming.	89%
Understanding of commercial nature and imperatives of most social media sites.	95%

As hate speech on social media increases (it is “shockingly easy” to find, according to the Commons Home Affairs Committee – gu.com/media/2017/may/01/social-media-firms-should-be-fined-for-extremist-content-say-mps-google-youtube-facebook), worries about online gambling proliferate and more and more schools report younger and younger pupils playing 18-rated games with the tacit blessing of parents, this is a key topic to explore with young people.

In my school

Why not carry out an anonymous survey of the games pupils play at your school and the social networks they are on, asking about things that have gone wrong and dangers they have spotted? There will be plenty to discuss – with pupils and with colleagues!

Resource tip

Check out the resources we have curated for you at gaming.lgfl.net or social.lgfl.net – ‘Play Like Share’ is great for KS2, the PEGI site has information about game age ratings, and there is plenty of advice for parents, such as guides to commonly used apps.

Settings (77%)

Identification of risks in cyber-security situations.	50%
Safe use and maintenance of a secure Wi-Fi connection.	51%
Threat identification and strategies.	86%
Critical evaluation of the likelihood that an app or supplier is safe.	88%

TalkTalk, US Democratic Party, Tesco Bank, Yahoo… the list goes on. If some of the world's biggest organisations still fall prey to hacking, phishing, ransomware and other attacks at the heart of their cyber security, then how much protection has the average pupil got?

In my school

Show the 'Data to Go' video from LGfL's Cyber Security resource cybersec.lgfl.net (if you aren't in an LGfL TRUSTnet school you won't be able to access the entire resource but can find the standalone video on YouTube – search 'Data to Go CIFAS'). Do your pupils know their privacy settings and who can see their posts… and other data (Instagram geolocation setting is a good place to start)?

Resource tip

Have you shared resources from parents.lgfl.net with parents at your school? There are lots of great resources, but make sure they know Internet Matters to help with their home internet settings and app guides including the from NSPCC (including their great app about apps - NetAware).

Talking (77%)

Knows difference between and appropriate use of CC and BCC	49%
Can use and manage contact lists	62%
Is aware of strategies to ensure webcam use is "safe"	87%
Can identify email scams (various) and apply appropriate actions	93%

“Nobody uses email anymore”, or so they say. But in nearly every office they do, and whilst this *may* not be the case when many pupils reach working age, these skills remain for now very important and worth training with pupils… even if many adults believe that bcc is designed to surreptitiously ‘drop colleagues in it’ as opposed to protecting email addresses.

As for recognising scam, phishing, grooming or otherwise genuine contacts online, whilst the results are encouraging, the increase in phishing attacks on businesses, schools and individuals means that we need to remain vigilant in training young people for this area.

It is good to see that pupils have been hearing messages about webcam use; however, given recent incidents of grooming and sexual exploitation via live streaming apps (compounding the ongoing situation surround random video chat apps), there remains much work to be done in this area

In my school

A great way to encourage pupils to see their teachers as credible in the online safety area is for teachers to admit to their mistakes. Why not tell your pupils about a time you got something wrong online to encourage them to be honest and think about what and who they believe or not – and why?

Resource tip

The sharing activities within the Trust Me resource for developing critical thinking online are excellent for spotting scams and genuine messages (of all sorts) – trustme.lgfl.net; there is also plenty of advice on the seemingly old-fashioned medium of email (search for email at messaging.lgfl.net).

Privacy (70%)

Explanation of their and others' (permanent and ongoing) digital footprints, and their impact on people's offline reputations.	33%
Identification of URLs which are safe for personal data entry.	42%
Explanation of location-based service and app-specific settings to turn on and off.	80%
Identification of factors that make a strong password.	94%

By default, anyone can view your profile and posts on Instagram; and geotagging is turned on by default (so pics from your bedroom and school are linked to the map and not hard at all to trace). It is therefore encouraging to see that pupils are aware of location settings. Whether this awareness is translated into action is another matter and worth pursuing with your pupils.

In my school

Further to this, rather than lecturing pupils on privacy settings and the potential future impact of their digital footprint (often ignored or not entirely believed), you might want to show them a news article of a teacher sacked on the basis of their social media presence (best for obvious reasons to choose an example yourself rather than ask them to Google sacked teachers!). For example metro.co.uk/2017/04/01/teacher-suspended-after-posting-provocative-selfie-on-facebook-6546910 or dailymail.co.uk/news/article-1354515/Teacher-sacked-posting-picture-holding-glass-wine-mug-beer-Facebook.html Do they think this is fair? Would they have expected it to happen (the teacher in the second article said that she thought all posts were set to private).

Resource tip

There are some great resources at reputation.lgfl.net which are useful for pupils (and your school!).

Money (2nd weakest area – 59%)

Identification of the hallmarks of a secure site (padlock, https, valid certificates).	45%
Knowledge of actions to take if in receipt of a phishing message.	51%
Identification of "real" cash transactions versus "not real" ones.	68%
Knowledge that URL names (e.g. of a bank) are not an indication of authenticity.	69%

The strongest and weakest competencies in the 'Money' theme are worrying and encouraging in equal measure. Teaching pupils about money matters is often taught as part of PSHE, and it is critical that online matters are embedded at the heart of money education. Matters such as recognising secure sites are relatively easy to teach but have with costly consequences of not knowing.

In my school

Why not ask pupils to use one of the resources from one of the high-street banks such as this quiz from Barclays (http://www.barclays.co.uk/security/digitally-safe-quiz) to start a discussion at home with parents and carers about some of the issues that will affect them all?

Resource tip

There are great tips, pages and videos on creating a strong password at passwords.lgfl.net, and of course the money section of CyberPass itself is very helpful (cpinfo.lgfl.net).

Looking (weakest area – 54%)*

Identification of effective searching skills.	**19%**
Selection of various "signs" (visual literacy) to indicate nature of risk.	**38%**
Understanding that the veracity/accuracy/currency of online content is not controlled by anybody in particular.	61%
Review of options and selection of "trustworthy" sites (critical evaluation).	69%
Identification of appropriate action to be taken if confronted by inappropriate content.	**76%**
Identification of basic settings within a search engine.	**84%**

"Let me just Google that!" How often do you hear or utter those words? Given the experience gained from extremely high frequency usage, one would hope that young people might understand some of the basic tenets of search. These results would indicate that this is perhaps not the case and that education needs to fill these gaps much more effectively, whether in terms of process, identification skills and settings, or critical analysis of information.

In my school

With the youngest pupils who have yet to learn safe searching skills, remember there are safe search engines available – Swiggle and Primary ICT Safe Search, for example. Remember that even when you are confident in your school's filtering and monitoring, theses might be useful tools to encourage so that pupils can then use them at home where parental controls may be lacking on domestic networks. Find these and more at safesurf.lgfl.net

Via the same link, check out further tips for searching as well as 'Trust Me', which has a Primary and a Secondary pack including activities to analyse the results of a Google search – do you notice the little 'Ad' box that appears at the top of many searches?

Resource tip

With only 62% of pupils recognising that no-one in particular "controls the veracity/accuracy/currency of online content", it can only be fakenews.lgfl.net for some excellent resources in this area for different ages. And for staff as well as pupils, try the 'Blue Feed, Red Feed' tool from the Wall Street Journal!

** As this is the weakest theme, all 'Looking' competencies are included in this table.*

What next?

Success?

It would be simplistic to conclude that as a result of this data, online-safety educators can claim to have 'nailed' friendship and sharing (indeed, there is plenty of evidence to demonstrate that this is not the case). However, it is not appropriate to disregard the findings either. Resource providers such as LGfL and the other expert organisations referenced in this report need to examine the messages that are being propagated towards young people in this area and examine why the messages being received are not being translated into 'appropriate' action. And this self-analysis is just as, if not more important for teachers on the ground (we would love to hear from you at safeguarding@lgfl.net).

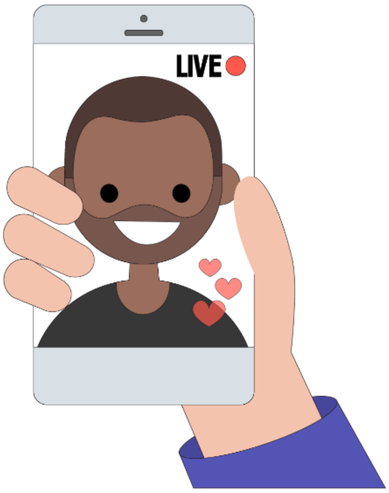
Failure?

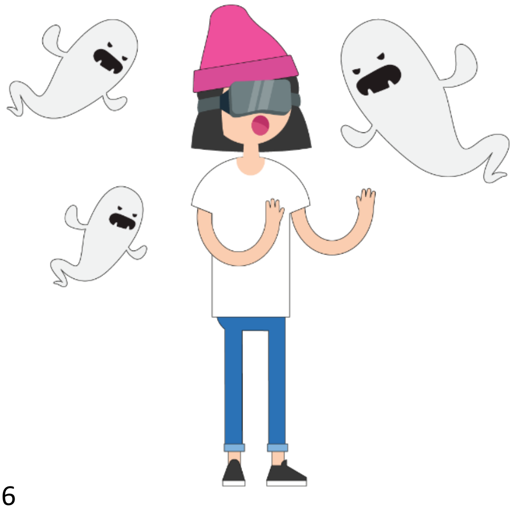
As the two weakest themes, Money and Looking (or searching) require further investigation in terms of the effectiveness of the resources available, as well as the extent to which schools dedicate time to these areas. Whilst teaching time is of course limited, it is incumbent upon us in an age of phishing and fake news to ensure that the young people in our care are prepared to face the inevitable nefarious challenges ahead of them in a way that does not impinge upon the brave new digital worlds they are forming. At LGfL we will take this as a spur for the future (and a timely confirmation of the relevance of our new Cyber Security resource – cybersecinfo.lgfl.net), as we aim to help teachers become more effective. We would also encourage the UK Government to provide more support in this area for young people to back up campaigns already launched to support adults.

Future!

Life in an online world moves at a frenetic pace, and support for areas which are as new to adults as to young people remains equally important and challenging. We trust that the information provided in this report proves as useful to you as it is to us as we continue to work to keep children safe.

During summer 2017, CyberPass quiz questions were updated. Minor changes were made to improve the clarity of existing questions, and new questions were added (within the framework of the existing competencies) to account for recent developments and scandals surrounding live-streaming and geo-locating functions within popular apps (see safeblog.lgfl.net posts about Snap Maps and Live.ly). These will help us to ensure that CyberPass continues to support pupils as they continue to encounter, embrace and shape new technologies before adults have even heard of them.





Appendix 1 – Full table of results according to competency

Row Labels	Correct answers	Total answers	& of correct answers
Friends			
Articulation of risks associated with meeting online connections in person and strategies to enact if doing so.	2679	3270	82%
Identification of and selection of options to address cyber-bullying and appropriate levels of escalation.	3130	3781	83%
Identification of and selection of options to address cyber-bullying of others and appropriate levels of escalation.	3126	3764	83%
Identification of cyber-bullying prevention strategies.	3020	3571	85%
Identification of the different forms of cyber-bullying versus other inappropriate (one-off) behaviour.	3341	4448	75%
Knowledge of how behaviour might be misconstrued as cyber-bullying and identification of indications from others that may be the case.	2814	3514	80%
Knowledge that all is not what it appears online and that sometimes people can use the web to make contact for "bad" reasons.	2492	3859	65%
Management of privacy settings and friending.	2870	4113	70%
Matching of behaviour to situations.	2814	3095	91%
Recognition of inappropriate behaviour and strategies to mitigate and manage the social ramifications of reporting and "unfriending".	2994	3286	91%
Strategies to address trolling.	2882	3182	91%
Friends Total	32162	39883	81%
Looking			
Identification of appropriate action to be taken if confronted by inappropriate content.	3379	4448	76%
Identification of basic settings within a search engine.	3145	3747	84%
Identification of effective searching skills.	1482	7615	19%
Review of options and selection of "trustworthy" sites (critical evaluation).	5828	8487	69%
Selection of various "signs" (visual literacy) to indicate nature of risk.	2034	5351	38%
Understanding that the veracity/accuracy/currency of online content is not controlled by anybody in particular.	2439	4009	61%
Looking Total	18307	33657	54%

Money			
Identification of "real" cash transactions versus "not real" ones.	**2511**	**3671**	**68%**
Identification of a one-off transaction as opposed to an ongoing commitment.	**3391**	**5212**	**65%**
Identification of phishing/scam e-mail/scams.	**2408**	**4134**	**58%**
Identification of the hallmarks of a secure site (padlock, https, valid certificates).	**2036**	**4520**	**45%**
Identification of ways to pay for in-app purchases.	**1870**	**3353**	**56%**
Knowledge of actions to take if in receipt of a phishing message.	**2001**	**3900**	**51%**
Knowledge that URL names (e.g. of a bank) are not an indication of authenticity.	**2377**	**3438**	**69%**
Money Total	**16594**	**28228**	**59%**
Playing			
Assessment of what happens to data posted to various websites.	**2868**	**3654**	**78%**
Explanation of the nature of online and offline games, and of how and when even offline games access the Internet to share information.	**2691**	**4056**	**66%**
Identification of content/info that should never be shared online.	**3035**	**3629**	**84%**
Identification of risks associated with online gaming.	**2769**	**3240**	**85%**
Identification of risks associated with posting personal data relative to the nature and reliability of the site.	**3251**	**3759**	**86%**
Identification of suitable and unsuitable usernames which might attract unwanted attention.	**11109**	**15823**	**70%**
Identification of the basic etiquette surrounding distributing images of others.	**2620**	**3618**	**72%**
Identification of the features of a high-quality, safe and secure social network.	**4163**	**5390**	**77%**
Identification of the risks associated with 'tagging', 'sharing', or otherwise distributing images of themselves or others online.	**3893**	**6226**	**63%**
Knowledge that all data on the Internet is permanent.	**2439**	**4186**	**58%**
Knowledge that all posts can be manipulated (edited, forwarded, tagged, shared, etc.).	**3009**	**3568**	**84%**
Knowledge that data posted to the Internet affects reputation (potentially negatively).	**2913**	**3556**	**82%**
Knowledge that in most cases social networks are self-moderated and require users to report inappropriate behaviour.	**3052**	**4045**	**75%**
Knowledge that people have the right to refuse "connection" and the rude or potentially criminal nature of chasing someone for this.	**2816**	**3326**	**85%**
Risk minimisation strategies for online gaming.	**2996**	**3349**	**89%**
Understanding of commercial nature and imperatives of most social media sites.	**17952**	**18934**	**95%**
Understanding that users of social media sites have a responsibility to behave in an acceptable manner.	**2924**	**6045**	**48%**
Playing Total	**74500**	**96404**	**77%**

Privacy			
Correct identification and explanation of a cookie.	3331	6146	54%
Explanation of location-based service and app-specific settings to turn on and off.	5602	7023	80%
Explanation of their and others' (permanent and ongoing) digital footprints, and their impact on people's offline reputations.	2375	7179	33%
Identification of factors that make a strong password.	24050	25501	94%
Identification of information that should never be shared online (unless with explicit parental intervention).	3486	5384	65%
Identification of potentially untrustworthy sites/messages and "likely" threats.	3927	5406	73%
Identification of URLs which are safe for personal data entry.	3193	7547	42%
Knowledge of browser privacy settings that must be set by users.	6076	9127	67%
Knowledge of privacy settings and their management across multiple apps/settings.	3951	7000	56%
Knowledge of the permanence of personal information shared on the Internet and others' ability to share this at will.	3794	5156	74%
Strategies to minimise likelihood of "infection" or scam.	4375	5706	77%
Understanding of need to seek permission BEFORE posting anything about anyone else.	3376	4999	68%
Privacy Total	67536	96174	70%
Settings			
Critical evaluation of the likelihood that an app or supplier is safe.	12194	13789	88%
Identification of risks in cyber-security situations.	4338	8760	50%
Knowledge of individual mobile app setting required to maintain security.	3500	4836	72%
Matching of threats and effects.	33100	39634	84%
Reasons for security on personal mobile devices.	3315	6237	53%
Safe use and maintenance of a secure Wi-Fi connection.	3254	6353	51%
Threat identification and strategies.	23298	27071	86%
Threat prevention and minimisation strategies.	11101	15192	73%
Understanding of location-based settings, potential risks and what LB is.	4682	5976	78%
Understanding of security software and browser updates as key prevention tool.	4060	5358	76%
Settings Total	102842	133206	77%

Share			
Ability to make a 'mash-up' with appropriate permissions.	2839	4006	71%
Awareness of consequences to posting/downloading copyright protected content online.	3009	3578	84%
Identification of different labels attached to other people's content (CC, ShareALike, etc.).	3853	5085	76%
Identification of inappropriate postings.	3090	3780	82%
Identification of online content that has copyright attached.	3215	4036	80%
Identification of plagiarism and its inappropriateness.	3062	4314	71%
Identification of the ramifications of breaking the rules.	3431	3853	89%
Knowledge that school ICT environments (and others) are monitored.	3091	4323	72%
Recognition that "good" or "appropriate" behaviour is just as important online as it is offline.	3070	4168	74%
Understanding of the permanence of posted content, whether deleted or not.	2796	3834	73%
Understanding of what an AUP covers.	5529	6600	84%
Understanding that the use of Snapchat or Skype does not preclude images from being stored on the Internet.	2899	3419	85%
Share Total	39884	50996	78%
Talking			
Can identify email scams (various) and apply appropriate actions	2682	2893	93%
Can tell the difference between genuine messages in online chat forums and ones that are likely to be scams or other unwanted contact, and knowing how to respond/ ignore.	2734	3166	86%
Can use and manage contact lists	2561	4106	62%
Is aware of strategies to ensure webcam use is "safe"	2646	3048	87%
Know that all messages conveyed via connected technologies are permanent	2561	3400	75%
Know that attachments and/or links in emails can possibly be bad	9634	12183	79%
Knows difference between and appropriate use of CC and BCC	2634	5342	49%
Knows that WC can be recorded and posted outside their control	2682	3374	79%
Knows the posting images of others is potentially illegal (and irresponsible/unfair)	2591	3100	84%
Understand that the distribution of images and video is getting easier online and that controlling who sees anything online is very difficult	7066	8459	84%
Talking Total	37791	49071	77%
Grand Total	389616	527619	74%

More information about the CyberPass resource:	cpinfo.lgfl.net
Online-safety resources for parents, teachers and pupils at	osresources.lgfl.net
Subscribe to our blog at	safeblog.lgfl.net
Sign up for a fortnightly newsletter for DSLs and OS leads	safenews.lgfl.net
Follow us on Twitter	@LGfLDigiSafe
Like us on Facebook	facebook.com/LGfLDigiSafe