OPEN
RIGHTS
GROUP

Open Rights Group response to Age Appropriate Design Code of Practice Consultation

19 September 2018

Open Rights Group is a UK based digital campaigning organisation working to protect the rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.

We want a world where we each control the data our digital lives create, deciding who can use it and how. We want the public to fully understand their digital rights, and be equipped to be creative and free individuals. We stand for diverse participation in culture.

Summary

- Open Rights Group supports higher default privacy settings for children, in particular a restriction on behavioral advertising and data processing that leads to extended user engagement.

- Open Rights Group does raise concerns regarding the application of the age brackets in practice, in particular if it would create the need for age verification on sites which would have negative outcomes for children, calling for purpose limitation and data minimisation standards to be clearly set out.

- Open Rights Group encourages child data impact assessments, where children are consulted by online services on the clarity of the information they present to children to explain what the service does with their personal data.

- Open Rights Group calls for the Code of Practice to set out a clear set of principles for improving information given to children and parents about the level of data processing the service undertakes.

- Open Rights Group calls for the code to also seek to build the capacity of children to understand their rights, by building in parental consent counter-signing, and investing in education.

Introduction

Recital 38 of the General Data Protection Regulation recognizes that children merit "specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."[1] The recital goes on to make specific reference to the collection of personal data for marketing or user profiles or for services offered directly to a child.

The recital lays out that children should be considered differently to the adults online. It is an uncontroversial observation that rarely is the distinction made online between an adult and a child in a meaningful way. This is particularly true when it comes to privacy. Services targeted at children process data in similar ways to services that are mixed or targeted at adults.[2]

The Age-Appropriate Design Code of Practice provides an opportunity to fix that imbalance. It can address the relationship a child has with online services by creating stronger default settings and working towards better provision of information to children about terms and conditions and privacy notices. It can also operate as a learning experience, preparing children for adulthood as effective participants online with agency and confidence in their rights.

Achieving both of these outcomes require different approaches. With the former, tighter controls on data processing of online services, and a duty to conduct child impact data assessment's that include consultation with children would seem reasonable. On the latter, we need to seek a system that does not create a completely unrealistic digital life for under-18s that is quickly stripped away and replaced with the

[1] Recital 38, General Data Protection Regulation, http://www.privacy-regulation.eu/en/recital-38-GDPR.htm

[2] Global Privacy Enforcement Network Sweep 2015, https://www.garanteprivacy.it/documents/10160/0/GPEN+Privacy+Sweep+2015.pdf - found that sites were failing to provide privacy policies sufficient information to children, over-collection of information, and disclosure of information to third parties for vague purposes.

online experience of an adult. There are steps that need to be taken, in terms of capacity building, that the Code has to actively seek out so children can become effective participants online and can exercise and understand their rights online as they move into adulthood.

It is also important to make clear what data protection, and this Code of Practice, can achieve. It addresses the relationship between an individual data subject (a child) and a data controller (an online service), the processing that takes place of the data subject's personal data, the basis for that processing, and the responsibility a controller has to that data subject and their rights.

It does not specifically address marketing or content regulation, nor should it. These other areas may be discussed in terms of the forthcoming ePrivacy Regulation[3]. The Code of Practice should not be used as a vehicle for either of these aims as the GDPR is simply not designed for these discussions.

Ages to be included

Open Rights Group does not have any specific concerns regarding the appropriateness of the age ranges to be included from a development needs perspective. We would seek to question how practical these age ranges will be for services to be delivered. The age ranges could be illustrative but making it too prescriptive may backfire in creating further data processing without suitable protections in place or remove the opportunity for children to appear on a service altogether.

If the code would require data controllers to know which of their users exist in these brackets, how would they do this proportionately, meeting the data minimisation standards which are important to uphold?

Granular age verification would require the data controller to collect and process specific data, perhaps giving more insight for behavioral advertising, unless it is explicitly restricted. That would be an ironic twist to a code of practice that seeks to improve privacy standards and undermines it by requiring granular age verification that leads to granular profiling.

Verification of age, if it were to be meaningful, requires attributes for verification. Children before they receive their driver's licence would only hold their birth certificate or a passport as identity attributes. Requiring these to be provided before accessing an online service is a disproportionate burden, and in terms of passports which are expensive[4], leads to digital exclusion based on family income.

[3] ePrivacy Regulation https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation
[4] Get a child a passport, UK Government, https://www.gov.uk/get-a-child-passport.

Additionally, if the burdens were too great on the online services, they may decide to remove or restrict access to their service when previously they offered it. This has been seen with the General Data Protection Regulation in other areas.[5] While these services may be acting in error, the effect is the same, a restriction of access to information and it should be considered that the proportionality of rules in this sector can have extreme responses.

Recommendation on age brackets:

- Data minimisation and purpose limitation design standards in the code of practice clearly sets out that the age of a user is only to be used for verification purposes, and not for further processing for tracking, or profiling purposes.
- Users should not be required to verify themselves at the granular level of the age brackets.

Principles to consider from the Convention of the Rights of the Child

The principles contained with the Convention of the Rights of the Child that should be considered when designing the Code of Practice are:

Article 12 – The right of a child to express their views in all matters affecting them.

The Code of Practice could touch on a number of areas addressing Article 12:

Child data impact assessments

Where online services are specifically or likely to target children the data controller should undertake an additional impact assessment, beyond the mandatory Data Protection Impact Assessment that includes seeking the views of children. The assessment could include: the clarity of the consent framework the service operates, the ability of the child to understand and activate the rights.

Counter-signing in parental consent

Research shows that children have an instinct towards their privacy, with younger children seeking a greater privacy than older[6]. This could be reflected in their own consent for processing. While parental consent is a legal requirement for children

[5] 'Unroll.me to close to EU users saying it can't comply with GDPR', https://techcrunch.com/2018/05/05/unroll-me-to-close-to-eu-users-saying-it-cant-comply-with-gdpr/.

[6] The I in Online: Children and Online Privacy Survey, 2011, pg. 13. The I in Online is provided attached to this response as it is unavailable online.

under the age of consent, those children should still be given the opportunity to counter-sign having had the information presented to them in an intelligible form. If the child objects to processing, the parent, if they had previously consented, should be notified of the wishes of the child.

Article 13 – Freedom to seek, receive and impart information and ideas of all kinds.

The Code of Practice should consider sensitively the effect a disproportionate regulatory regime may have on a child's right to seek, receive and impart information. Creating an environment where online services do not offer their services, which some have done since the General Data Protection Regulation came into force, would be a negative outcome for the child's right to seek, receive and impart information.

Article 16 – The right to privacy.

Behavioral advertising

Behavioral advertising is shown to be particularly persuasive to children[7]. The basis of targeted advertising is an increased processing of personal data. The Code of Practice could restrict the opportunity for data controllers to perform behavioral advertising on children's personal data.

Recital 38 also suggests that children "merit special protection", in particular "the use of personal data of children for the purposes of marketing or creating personality or user profiles."[8] The Code of Practice could make definitive statements about this "special protection" may include. Practically, we should see a great respect for Article 16 as a result of the Code of Practice.

Verification, not profiling

In seeking to identify a child online the Code of Practice must deal delicately with verification requirements. Verification may be necessary to confirm a child is under the age of consent, or under 18, but it should not be used for further profiling of the user. If such a practice were to occur this would have a negative impact on Article 16 rights.

Article 17 – The right to access to information and material from a diversity of national and internal sources.

Accessing information from a variety of sources speaks to the Code's need to deal delicately with the proportionality of the design standards imposed. Online services

[7] Digital Childhood: Addressing Childhood Development Milestones in the Digital Environment, pg. 16, https://5rightsframework.com/static/Digital_Childhood_report_-_EMBARGOED.pdf.

[8] General Data Protection Regulation, Recital 38, http://www.privacy-regulation.eu/en/recital-38-GDPR.htm

that may restrict access due to a heavy-handed design regime would be a negative outcome for Article 17 that should be avoided.

Article 27 – The right to a standard of living adequate for the child's physical, mental, spiritual, moral and social development.

The right to social development includes the right to access and experience the Internet. The Code should operate to give children the tools to enjoy social development and be in control of their personal data. The code should also seek to help them develop their skills online by seeking learning and capacity building opportunities to improve their understanding of their rights.

In addition, the right to social development applies to all children equally. Any measure that would require identity attributes so granular or specific that a child is unable to meet those by lack of resources (for instance requiring a passport or identity verification) would be a negative outcome for Article 27 and should be avoided by the code.

Open Rights Group would also recommend considering the work of the Article 29 Working Party[9], now known as the European Data Protection Board.

On aspects of design of code of practice

Default privacy settings for children should be set at a higher level.

It is a stated intention of the General Data Protection Regulation in Recital 38 that children merit special protection. On a practical level, this would mean their privacy settings are different to that of adults. Specifically, their default privacy settings should be set at a higher level.

The wish for high default privacy settings is also reflected in research that shows that children of younger ages believe they should have higher default privacy settings.[10]

Restriction on behavioral advertising and data processing for extended user engagement

[9] In particular 'Opinion 2/2009 on the Protection of Children's Personal Data (General Guidelines and the Special Case of Schools) WP 160', 11 February 2009.

[10] Footnote 6. I in Online is provided attached to this response as it is unavailable online.

Efforts to extend user engagement have an outsized effect on children. There is already a social incentive to be connected and interacting[11] with peers that adding a layer of technological incentivization has lead to concerning outcomes. Research conducted by YoungScot from last year showed the majority of children agreed they couldn't live without their devices, with an even higher number believing that some products have been designed to be addictive, and a significant portion feeling that these factors contribute to sleeplessness.[12]

Restricting data processing for extending user engagement could remove one of the driving factors contributing to a perceived need to have devices available and an "always on" mentality.

Behavioral advertising is a tool to develop targeted advertising based on the browser habits of individuals. The United States Federal Trade Commission has taken the approach to require affirmative parental consent before behavioral advertising of children's data can be conducted.[13] The Age Appropriate Code of Practice should go further.

It is difficult for parents, let alone children to understand behavioral advertising.[14] Parental consent may not be an appropriate model for seeking to process this data, and further the processing of this data fails to meet the Recital 38 statement of seeking "specific protection" for children. As the Working Party 29 suggested in an opinion from 2013[15], data controllers should not process children's data for behavioral advertising purposes. The Code of Practice should make that recommendation a standard.

Consult with children (not just parents)

The parental consent model operates only when a child doesn't have capacity to give consent on their own terms, this means anyone under the age of 13 in the UK (12 in Scotland). That model requires a parent to sign off on the data processing that is to take place. However, the appreciation of privacy may be drastically different between

[11] Boyd and Marwick, Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies, pg. 8 – 9, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925128.

[12] Our Digital Rights: How Scotland can realise the rights of children and young people in the digital world, , 2017, pg. 38, https://www.youngscot.net/wp-content/uploads/2017/05/Five_Rights_Report_2017_May.pdf.

[13] Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[14] Why Parents Help their Children Lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act', 2011. https://journals.uic.edu/ojs/index.php/fm/article/view/3850/3075

[15] Article 29 Data Protection Working Party, Opinion 02/2013 on apps and smart devices WP 202', 27 February 2013, https://www.pdpjournals.com/docs/88097.pdf.

parent and child and purely parental consent may miss the learning opportunity that is presented.

Parental consent is a model that operates on the basis that parents (1) have a good grasp of privacy notices (2) are sensitive to their children's development needs online and (3) have a realistic assessment of risk for their child in using these services.

Arguably parents fail on all 3 of these areas continuously. In particular research has shown that parents are not understanding of how children use online services[16], can overreact to misunderstood contexts[17], and are at risk of 'consent fatigue'[18] leading to clicking without thinking.

To achieve the learning and capacity building outcome that Open Rights Group supports for the Code of Practice, there should be a requirement for joint consent between the parent and the child. This gives the child responsibility and an insight into agency that is waiting for them in adulthood, while also providing the necessary guardian approval for children under the age of 13.

The Dutch Data Protection Authority, in guidelines from 2007, pointed out a social responsibility of the website owners under the age of 16 to explain the rights and obligations of their users in a clear and understandable language. This was despite the fact the legal requirement only extended to receiving the consent of the parents.[19]

If the parent consents, a notice should be sent to the child that allows them to also consent, in language that the child can understand, giving them the opportunity to also consent and exercise their right to express their views. If the child does not consent, another notice should be sent to the parent to notify

Parental consent does not build children's confidence in asserting their rights and may not protect their privacy. Encouraging counter-signing, joint consent or parallel consent achieves both aims of addressing the relationship between a data subject and a data controller and improving the agency of younger internet users.

Accessing and exercising rights

Article 13 of the General Data Protection Regulation sets out the information to be provided where personal data are collected from the data subject. In particular the

[16] Footnote 9 pg. 16.

[17] *Ibid*.

[18] Consent for processing children's personal data in the EU: following in US footsteps?', pg 171, https://www.tandfonline.com/doi/full/10.1080/13600834.2017.1321096.

[19] Dutch Data Protection Authority, 'Public of Personal Data on the Internet' (guidelines), December 2007, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/en_20071108_richtsnoeren_internet.pdf.

controller shall provide the data subject with information about exercising their rights.[20]

This means that regardless of the basis for processing, controllers dealing with personal data of children need to provide this information in a language the child understands to meet this.

There is a question about processing that relies on parental consent. In such circumstances should the child still be capable of exercising their data protection rights independent of parental consent?

The Code of Practice should seek clarity on the question, how should a controller respond to a request directly from a child whose data is being processed on the basis of parental consent.

Providing clear information

There is a clear need for a general improvement of providing clearer information to consumers, whether they are adults, children, or the parents of those children. Much research has gone into the length of notices[21] and how adults fail to engage fully with the consent process. Creating a burden or standards rating framework for clearer information for parents and children would go a long way to meeting the aims of the Convention on the Rights of the Child.

The Global Privacy Enforcement Network privacy sweep from 2015 looked at data processing and children, including the provision of information. The conclusions were concerning. They found that 78% of sites assessed failed to use simple language or failed to present warnings that children could easily read and understand.[22] This is an unacceptable rate and shows a disregard for responsibilities that the websites assessed have towards children.

Just as nutrition information has undertaken a revolution in clarity, data processing is due one. Efforts like Data Rights Finder[23] that try to summarise and highlight relevant information, or ranking systems like Who Has Your Back[24] offer a template that the Commissioner's code of practice could seek to emulate. Additionally, establishing

[20] General Data Protection Regulation, Article 13(2)(b) and (d)

[21] The Cost of Reading Privacy Policies, http://www.casos.cs.cmu.edu/publications/papers/CostReadingPrivacyPolicies.pdf , pg 17-18.

[22] GPEN Privacy Sweep 2015, https://www.garanteprivacy.it/documents/10160/0/GPEN+Privacy+Sweep+2015.pdf

[23] https://www.datarightsfinder.org/

[24]Who Has Your Back?, Electronic Frontier Foundation, https://www.eff.org/homepage-feature/who-has-your-back.

Childhood Data Impact Assessments should include a question on the clarity of information provided, including consultation with children on the language used.

A rating system could seek to articulate the level of data processing that takes place on the site, a level of privacy potentially, which can be easily understood and compared against other online services. It should also seek to show how the level of privacy is affected by the data subject choosing to restrict permissions for data processing.

Other examples of design

Friction in technology can drive people to very different outcomes. Deployed correctly with good usability, it can make people think about what a controller is doing with their data, and that is a good thing. Deployed incorrectly, it can result in people circumventing controls, leading to negative outcomes, or disabling controls altogether.

For example, Apple's parental controls on Macs block all https websites. The basis being that due to encryption, the content filter is unable to examine the content of a page and for that reason encrypted websites must be explicitly allowed. Considering the prevalence of https, and the benefit of SSL encryption, the friction created by the Parental Controls here are counterproductive.

It is against best practice and leads to friction and constant need for parents to unblock normal websites. Further, it could easily lead to parents disabling parental controls to save themselves, and their kids, the unnecessary friction[25]. This is bad design.

Additionally, we see where hurdles are placed to try and benefit children but are too low and not correctly constituted. Research shows that millions of parents in America avoid age bans on social media sites like Facebook by letting, or assisting, their child lie about their age.[26]

This is due to the binary decision online services have taken on their responsibility to data subjects. The sites too often are set on the premise that you are either over 13 and thus can consent and be treated as an adult, or under-13 and thus you can't consent and have too many regulatory burdens. The result is under-13's lying to get on Facebook and have their data processed as though they are adults.

[25] Mac OSX v. 10.5, 10.6: About the Parental Controls Internet content filter, https://support.apple.com/en-gb/HT201813 "***https* note:** For websites that use SSL encryption (the URL will usually begin with *https*), the Internet content filter is unable to examine the encrypted content of the page. For this reason, encrypted websites must be explicitly allowed using the Always Allow list. Encrypted websites that are not on the Always Allow list will be blocked by the automatic Internet content filter."

[26] Why parents help their children to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act', boyd and others, https://journals.uic.edu/ojs/index.php/fm/article/view/3850/3075

This is not an argument for establishing mandatory age verification requiring hard identity attributes. That would lead to negative outcomes we have laid out above such as digital exclusion and unfair burdens. This is an articulation of the problem that the code of practice should seek to solve: give children and their parents the opportunity to access online services honestly, resulting in age-appropriate experiences and information designed to enhance safety, exercise rights, and prepare the child for engaging online when they reach adulthood.

Beyond standards for data controllers

While better information provision and consultation with children on the wording of terms and conditions, and privacy notices would be useful in building up children's agency it would mean very little unless proper investment in children's ability to be competent, confident online actors is achieved.

This is achieved by doing more than setting standards for data controllers. It requires education at a proper level, from an early age and continuing throughout school years. Beyond the code of practice there should be a call for curriculum development that would achieve this.

The problems for children begin not at opaque wording in privacy policies but at the existence of privacy policies. Younger people appear unaware of what privacy policies are or where to find them. With a challenge such as this, it doesn't matter how much work is put into a privacy policy that is clear for multiple reading ages if a child doesn't know where to find a privacy policy, or to even know they should expect to see one on a service they visit, is concerning.[27]

The wish for greater education is evidenced also by children themselves. Consultations have shown an interest from children to learn more about how the internet and companies on the internet work.[28] These wishes should not be set aside.

Placing greater burdens on data controllers to operate with regard to children to one thing is a laudable outcome. Investing in educating children to gain a better understanding than their parents about the internet, the internet economy, and their rights online, has the potential to change society.

[27] The I in Online: Children and Online Privacy Survey, pg. 10.

[28] The Internet On Our Own Terms: How Children and Young People Deliberated About Their Digital Rights (January 2017), pg. 7 https://casma.wp.horizon.ac.uk/wp-content/uploads/2016/08/Internet-On-Our-Own-Terms.pdf.

ANNEX: The I In Online – Child Privacy Report: Young people's use of social technology and their attitudes toward Data Protection, 2011 the i in Online

Children and Online Privacy Survey

Child Privacy Report

Young people's use of social technology and their attitudes toward Data Protection

About The i in online

The i in online aims to educate primary school children aged 9-11 and secondary school children aged 14-19, their parents and teachers about using and providing their personal information online and also highlights the potential pitfalls of sharing too much personal information on the internet when using blogs or social networking sites such as Facebook, Twitter, etc, and not managing privacy settings effectively. Through interactive sessions, using PowerPoint and videos, legal experts highlight the regulatory and legal aspects of this topic, whilst also demonstrating technical issues and illustrating mechanisms to help protect personal data whilst using the internet. www.theiinonline.org

Background to Data Protection Day

On 28 January, The i in online had 135 presenters delivering 112 sessions at 82 primary and secondary schools in 16 different locations across the UK. Presentations and workshops were given to 6,260 school children for Data Protection Day on 28 January 2011. We were working alongside the Information Commissioner's Office and the Irish Data Protection Commissioner's Office, who are supporting the activities on Data Protection Day. We had Assistant Commissioners from the ICO, 110 law students from BPP Law School, academics from Plymouth University and legal professionals from Speechly Bircham LLP, Barclays, BBC and Field Fisher Waterhouse LLP involved in the event. The number of children involved in Data Protection Day went from 300 in 2010 to 6,260 in 2011.

Executive Summary

The i in online data provides a large population (4116 in total) analysis on the behaviours and attitudes of young people toward online technology and privacy. Some headline statistics confirm our beliefs around such matters:

- children and young people readily engage with online social media
- sometimes they struggle with the policies that are supposed to be in place to protect them
- they are aware of the need to protect their data, but are not always equipped to do so.

Our respondents were asked whether they engaged in any social networking activities themselves. In total 69% of our respondents said they did use social networking sites. There was some gender differences, with girls (72%) more likely to have a social networking profile than boys (65%).

The social network that is most popular is, unsurprisingly Facebook, with 47% of respondents saying they had a Facebook profile. Again unsurprisingly the vast majority of secondary school respondents (88%) had Facebook profiles. However, we also had over a third (39%) of young people of primary school age said they had Facebook profiles. Girls are slightly more likely (50% in total) to have Facebook profiles than boys (43%).

The second most popular social networking activity was MSN, with 20% of respondents using it. Girls are more likely (26%) than boys (15%) to use MSN. Somewhat surprisingly it was almost as likely for a young person of primary school age (21%) to use MSN as someone of secondary school age (27%).

Boys are also more likely (56%) than girls (33%) to have an avatar, a virtual representation of themselves. However, there is little evidence to show that having an avatar results in different behaviours or attitudes toward data protection.

Our respondents were asked whether they had ever read a privacy policy. In total 40% of respondents had, meaning 60% of young people have not read the privacy policies of the web sites they use. This statistic differed little between young people of primary and secondary school age, but girls were more likely (44%) than boys (35%) to read a privacy policy. Boys are likely to have a more relaxed attitude toward data and data sharing, although this is far from irresponsible with the vast majority still believing their data should only be seen by friends and family and parental consent was necessary all scenarios presented about where their data might be exposed.

When those who had not read a policy were asked why not, there were a variety of responses. 32% said they didn't know what a privacy policy was, with 23% saying they didn't know where to find it. A quarter felt they were too complicated, and another quarter did not feel it important. Interestingly more secondary school respondents (44%) felt they were too complicated, although more primary children didn't know what a privacy policy was (37%).

Those who had looked at privacy policies had divided opinions, with around half (51%) thinking they were easy to find and 57% understanding what was there. The vast majority (84%) looked at the policy because they thought it was an important thing to do. There was little statistical variation across the demographic groups for those who had looked at privacy policies.

So we had an interesting split in our population – those who do engage in privacy policies may understand what is presented and think they are important. However, the majority of our respondents hadn't seen a policy for a number of reasons. They were also asked what might be done to improve privacy policies and a large number of children said privacy policies should be made more simple with "less words".

However, it was also clear that our respondents felt that privacy on social networking was important, with the vast majority (85%) saying that social networks should have the strongest privacy settings by default and an even larger majority (94%) feeling that clear rules were needed to help with the removal of photos and videos posted without consent.

We can also show that under aged Facebook users are responsible with their data and show little variation in attitude with those who do not use it. In addition, they are more likely to read privacy policies (48.8% of primary Facebook users compared to 39.6% of the total primary population) and be aware of why they are important.

What our data does clearly highlight is the need for education at a primary school level. While the use of social networking used to be considered something for secondary aged pupils our data shows that the majority of primary aged pupils also engage. However, it also shows that primary aged pupils are potential more vulnerable as a result of not being aware of privacy policy or where to find it. While they are generally more protective of their data, the change in attitude at secondary age does suggest that without effective education at a primary school level, there is potential for more risky behaviours in adolescent life.

The data also shows that while not all of our population felt privacy policies were complicated there was a great deal of confusion around them. They were also very clear that service providers should provide the most private settings by default. Clearly this is a population that feels service providers also have a responsibility to protect their data, but also provide policy and advice in a clear, understandable, and easy to find manner.

In conclusion, children and young people are very much engaged with digital technology and its social uses. However, there are still significant issues around education and practice to be addressed. While our population did not come across as naive around data protection issues, they were clearly not as well informed as they could be, and felt they needed help from service providers in ensuring “their” data was protected.

The analysis of the data was conducted by Prof Andy Phippen, Plymouth Business School, University of Plymouth.

Headline Demographics

The responses in terms of gender and age are presented below:

Are you:

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	1945	47.3	48.1	48.1
	Female	2096	50.9	51.9	100.0
	Total	4041	98.2	100.0	
Missing	System	75	1.8		
Total		4116	100.0		

How old are you:

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	8-9	572	13.9	14.1	14.1
	10-11	2438	59.2	60.3	74.4
	12-16	1020	24.8	25.2	99.7
	17-18	13	.3	.3	100.0
	Total	4043	98.2	100.0	
Missing	System	73	1.8		
Total		4116	100.0		

Overall there was a balanced gender split, almost 50/50 once non-responses were removed. In terms of age ranges just over 1,000 responses were from young people of secondary school age, and just over 3,000 from primary children. The volume of this response presents us with a good opportunity to explore attitudes toward data protection among primary school children.

Survey Design

The survey was designed to collect information on both the use of technology by children and young people and their attitudes toward privacy and consent. Aside from the key demographic information, it was broken into three main sections:

1. Online behaviour:

- Do you use social networking sites? And if so which ones?
- Do you have an avatar?

2. Privacy policies and awareness:

- Have you ever read the privacy policy on a website (if yes/no, why?)

3. Attitudes toward online privacy:

- How would you feel if your profile was viewed by (friend, mum, teacher, etc.)
- Do you think privacy settings on websites should automatically be set to most private?
- Should websites provide clear rules on how to go about removing a photo or video on a website which has been published without permission?
- How old do you think you should be to consent the use of your personal information (when signing up to a newsletter, putting CCTV in school, etc.)

The remainder of this report explores this at a number of levels. Initially we will investigate responses to the questions across the whole of the population, as well as gender splits to consider different attitudes for girls and boys. Following this, we will consider the difference in behaviours between older and younger children. Finally, we will focus on a specific group of primary aged children, those that use Facebook. Given the issues surrounding the use of Facebook by children under 13, and the concerns of teachers and parents regarding this, our data provides us with a rare opportunity to compare the attitudes and behaviours of “under aged” Facebook users compared to a wider population. While there are not many differences between practices and attitudes of Facebook using and non Facebook using primary aged pupils, there are a couple of clear differences that do present a potential benefit for those who do engage.

The use of Social Networking by the population as a whole

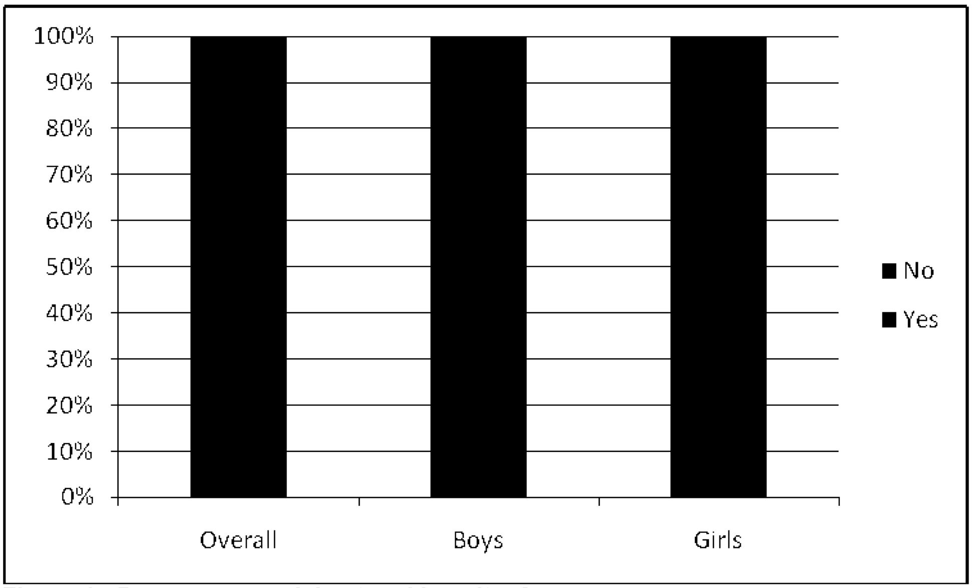

Figure 1 - Do you use social networking sites?

As can be seen from figure 1, the majority of our respondents used social networks of one type or another. While there was a slight gender difference between boys and girls (with girls more likely to use social networks), overall there is a consistent picture that the majority of young people use social networks.

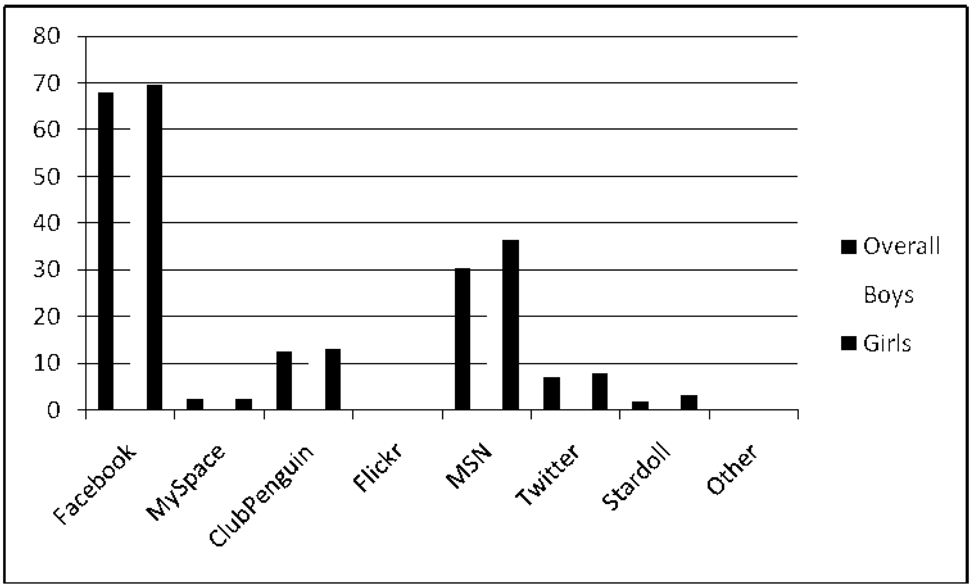

Figure 2 - If yes, which social networks do you use?

If we consider which social networks are used it is unsurprising to see that Facebook is by far the most popular with almost 70% of respondents using it. While there is a slight gender split with Facebook, it is most evident with MSN, where over 10% more girls use the service than boys. More exploration of these responses is conducted when comparing practice between primary and secondary children, as it is acknowledged that some service (for example Club Penguin) have a younger demographic than others.

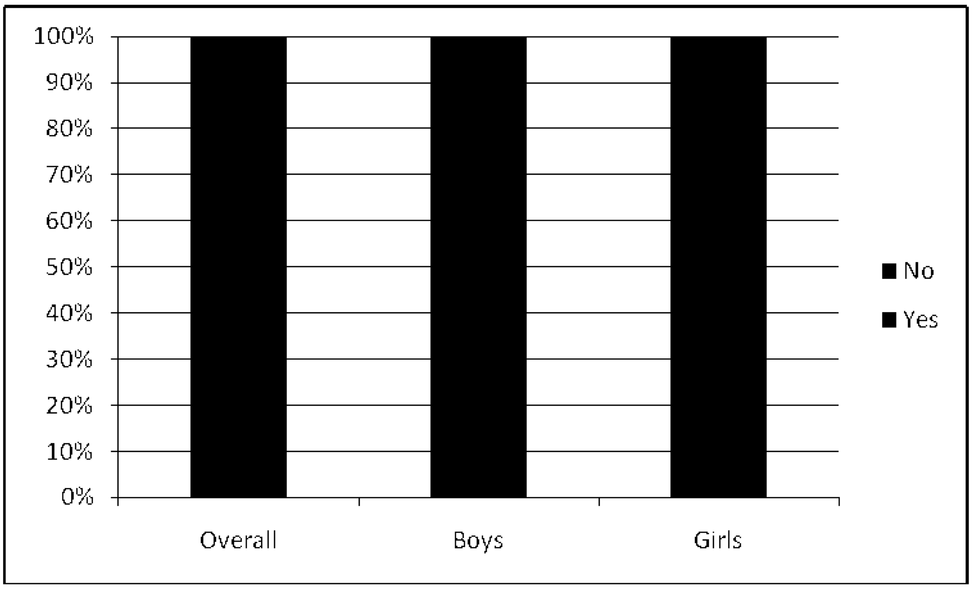

Figure 3 - Do you have an avatar?

A final "practice" based question asked whether the respondent had an "avatar" – a virtual representation of themselves in online worlds. Almost half of our respondents said they did, and there is a clear gender split with this question. This is unsurprising, given that avatars are closely linked to gaming sites and services and we are aware that more boys than girls engage with such. However, it is good to see data confirming opinion in this instance.

Privacy Policies and Awareness

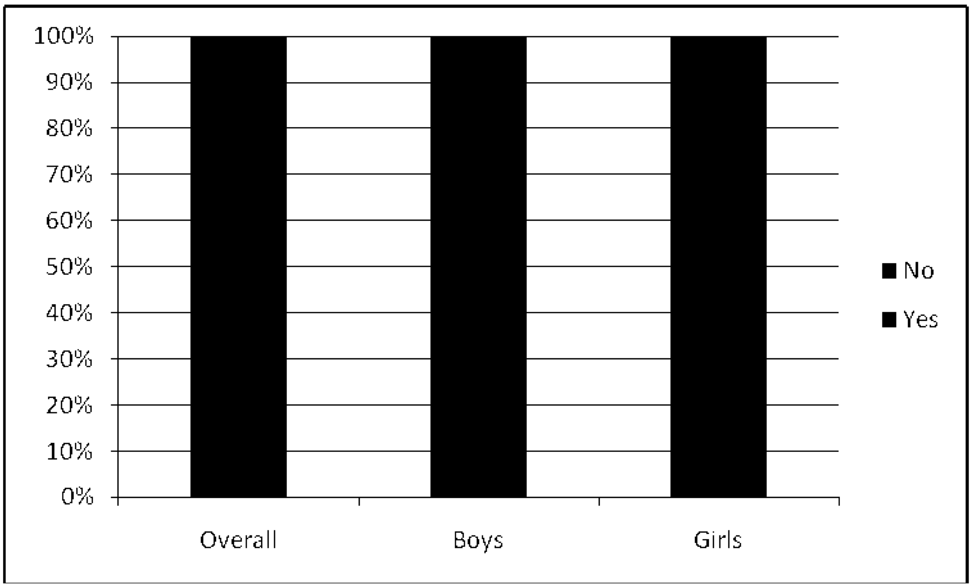

Figure 4 - Do you read the privacy policies on websites?

Clearly the results presented in figure 4 show are cause for concern. We have a population very much engaged in social networking and online activities yet less than half (only just a third in the case of boys) have ever read a privacy policy. When we isolated those respondents who said they did use social networking, the statistic only increased slightly, with 45% saying they had read a privacy policy. This means that over half of children and young people who use social networking sites do not consider the privacy policy before engaging.

If we consider the reasons why our respondents did not read privacy policies, there is no clear single reason. While we might hypothesise that the reason they aren't read is they are too complicated, in our responses only around a quarter said this was the case. What was more likely was to be they didn't know what is was.

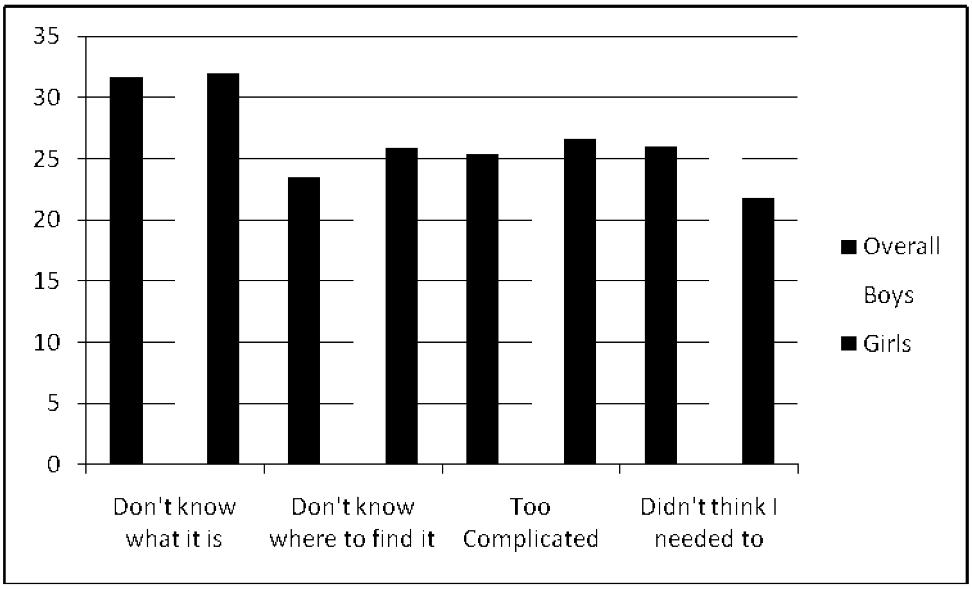

Figure 5 - If no, why not?

In contrast, those who had read privacy policies had done so because they thought them important. And, again, our respondents here show they did not find policies complicated to understand although almost half did say they did not think it was easy to find.

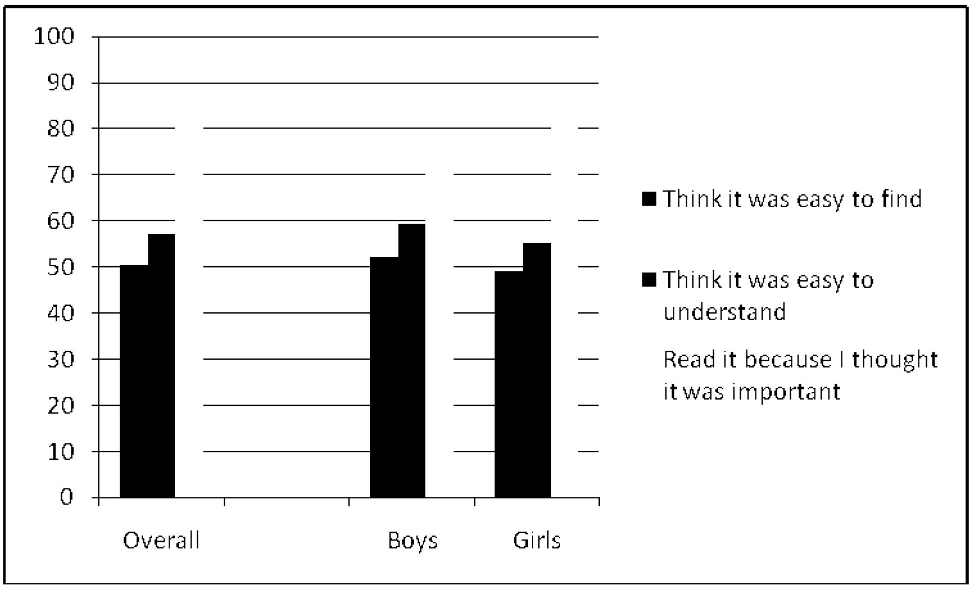

Figure 6 - If yes, did you...

From this level of analysis, we can develop a theory that privacy policies are ignored not because they are complicated, but because they are either difficult to find or there is a lack of awareness about what they are. We will return to these two issues later in the report.

Attitudes toward online privacy

The next series of graphs (figures 7-9) explore attitudes toward the sharing of our respondent's own data:

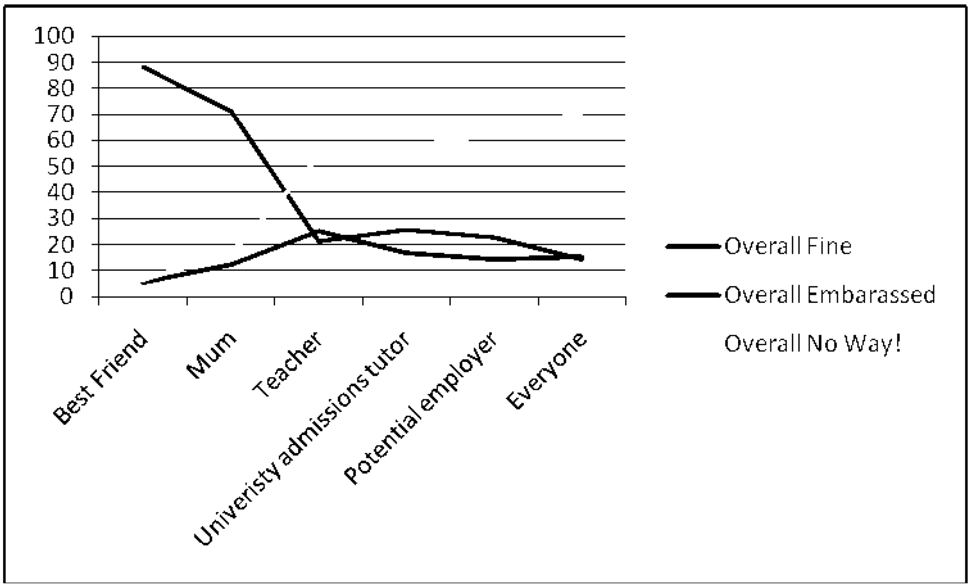

Figure 7 - Overall attitudes to social networking profile being viewed by various figures

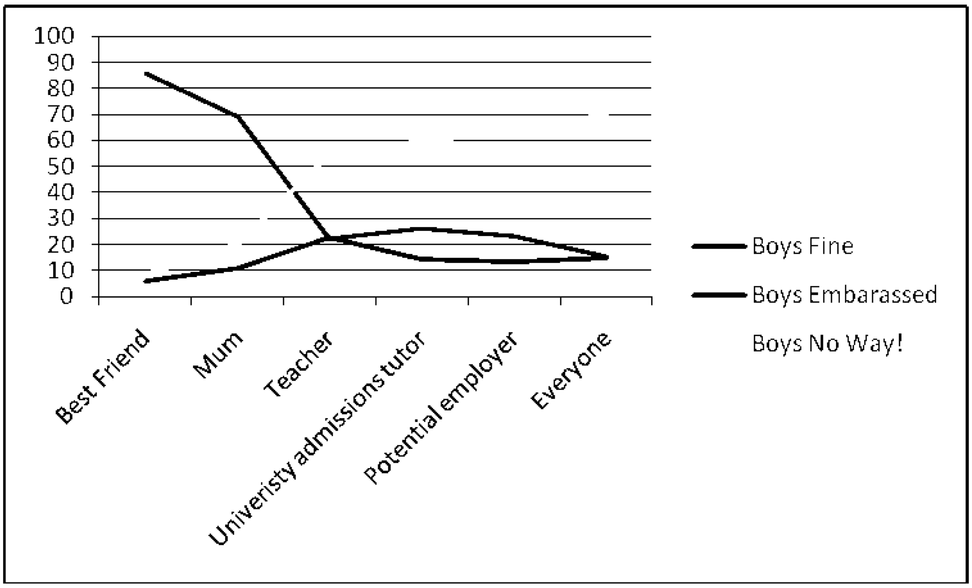

Figure 8 - Boys attitudes to social networking profile being viewed by various figures

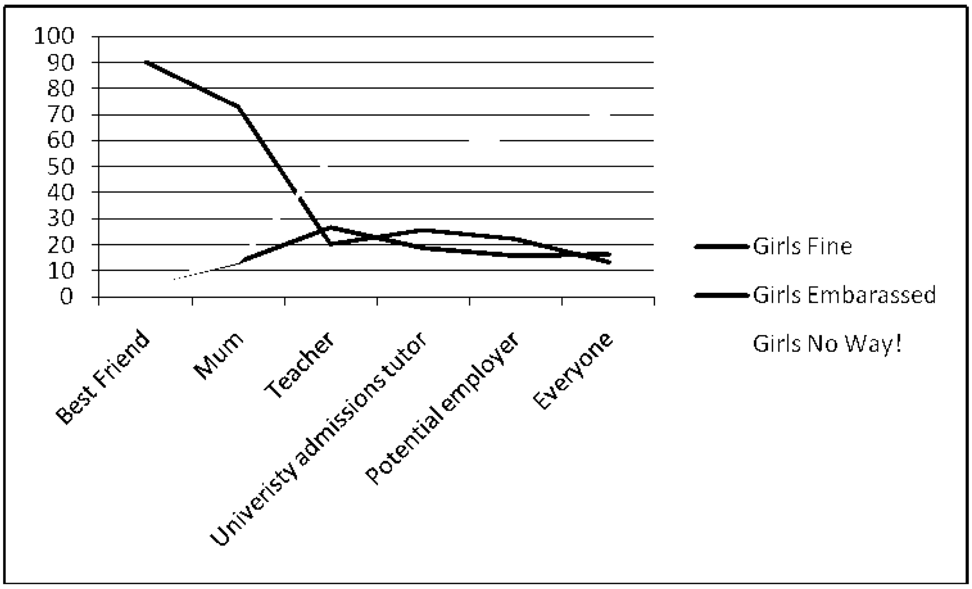

Figure 9 - Girls attitudes to social networking profile being viewed by various figures

Line graphs have been used to explore responses to illustrate trends around attitudes toward data sharing and privacy. It is clear that beyond friends and family data becomes precious to our respondents and they are not comfortable sharing it. There is some gender difference with boys, in general, being more open about their data than girls. However, there is a consistent pattern in all groups analysed.

Following on from this question, figure 10 shows that the vast majority of our respondents felt that social network providers should be responsible to provide settings that are “most private” by default. Again, there is a slight difference with boys being less concerned in the minority than girls. However, the vast majority in each group thought most private should be default and this shows a clear call to service providers to ensure users do not have to be solely responsible for protecting their data.

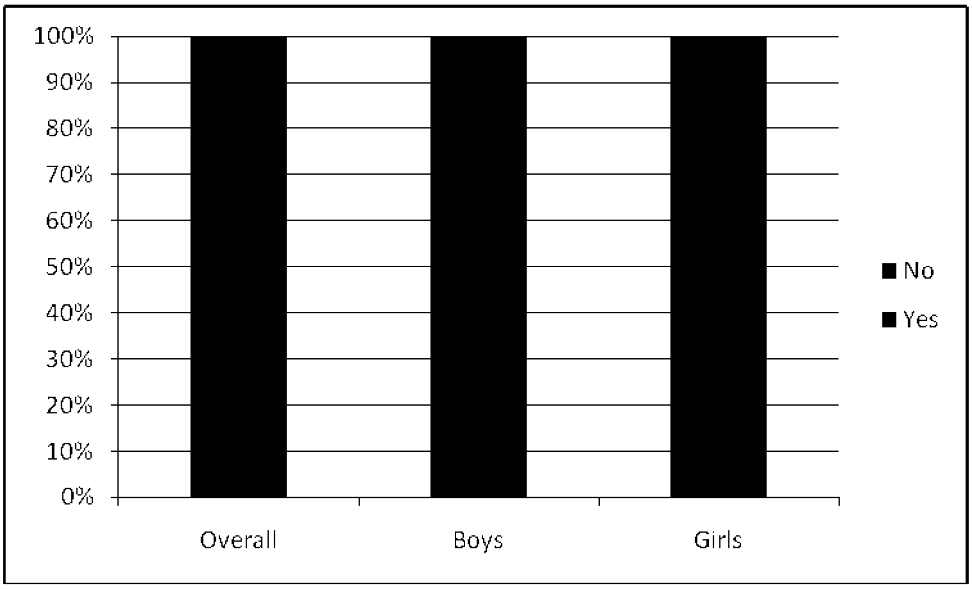

Figure 10 - Do you think settings should default to most private?

Finally, we asked our respondents to consider at what age consent should be able to be granted in different scenarios, illustrated in figures 11-13.

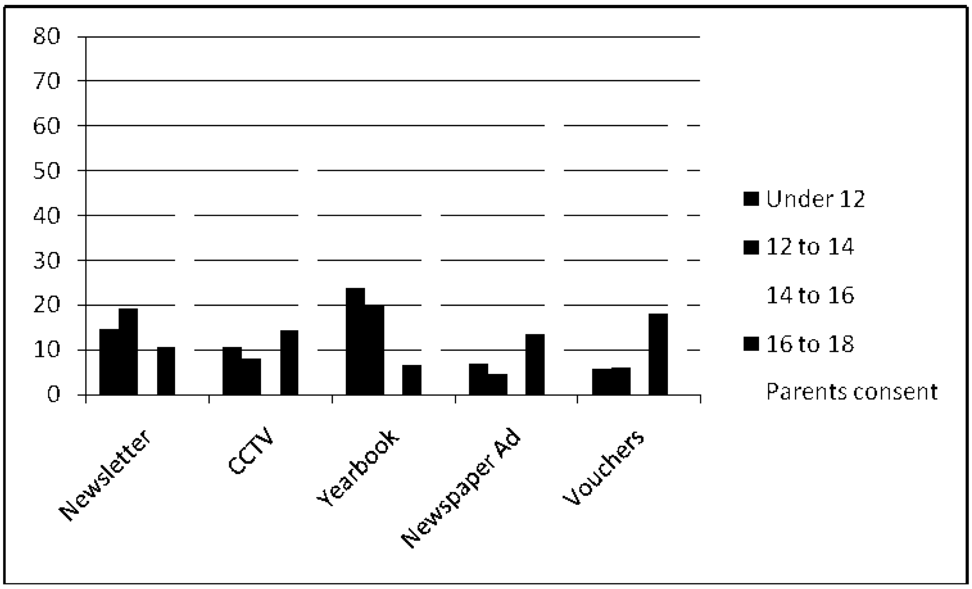

Figure 11 - Consent, overall group

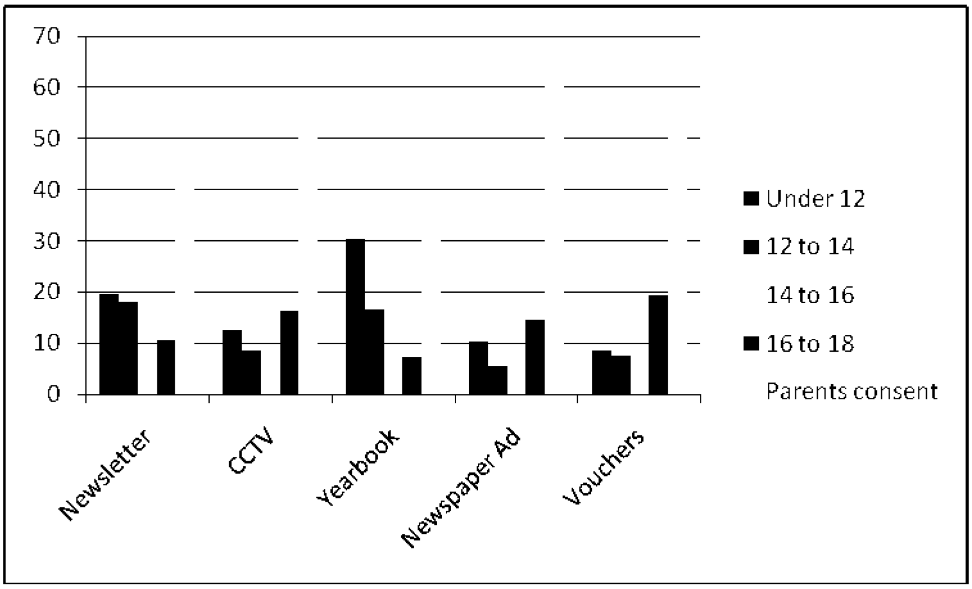

Figure 12 - Consent, boys

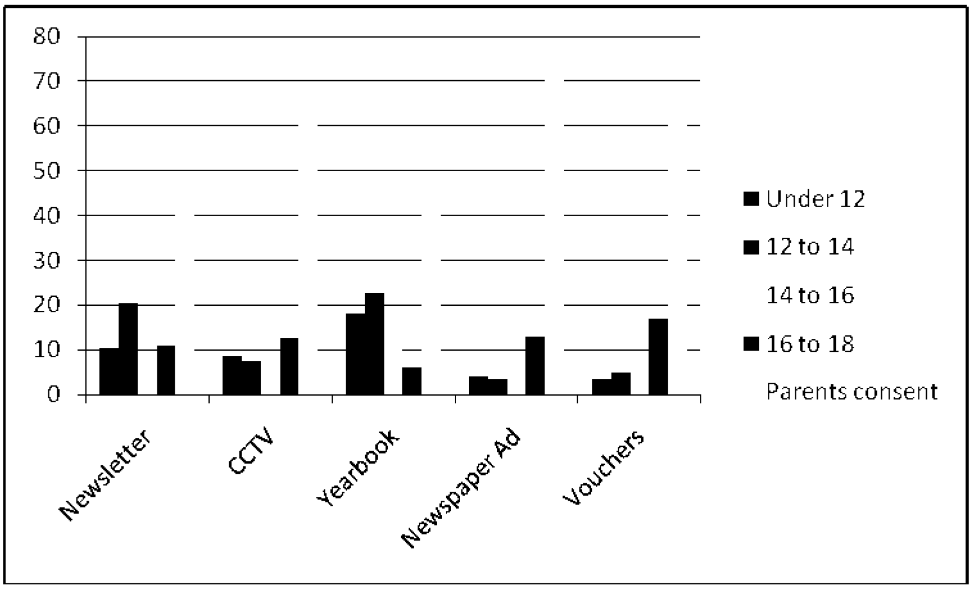

Figure 13 - Consent, girls.

In general, it is clear that the majority felt children and young people should not be responsible for consent, with the majority feeling parental consent was necessary in all scenarios. Again, boys show a slightly more relaxed attitude toward privacy, and in general have lower ages expectations than girls. Figure 14 provides an interesting illustration of this attitude, with a very similar pattern holding with the proportion of respondents thinking parental consent was necessary in scenarios:

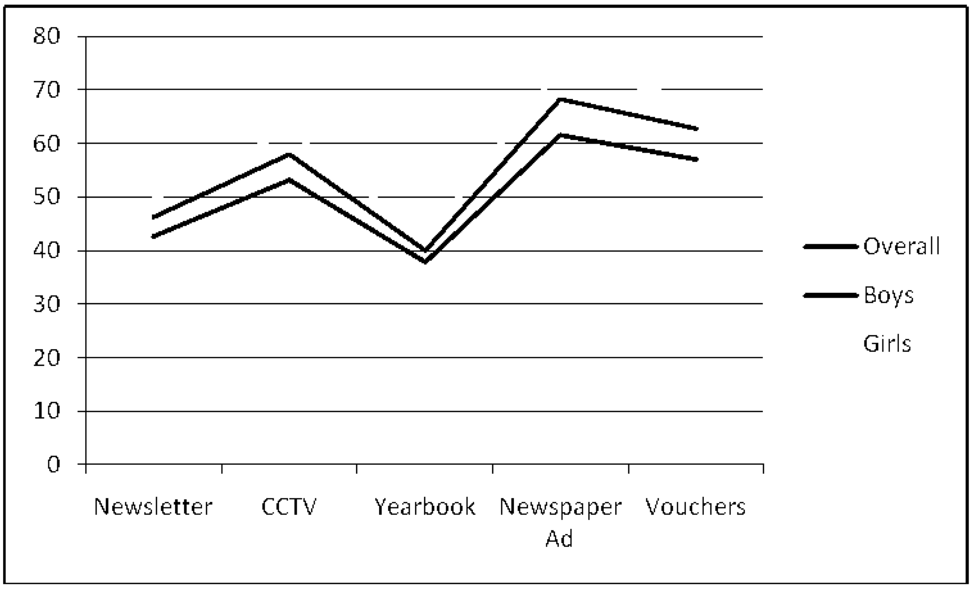

Figure 14 - Comparison, parental consent only

Primary/Secondary Comparisons

The second major piece of comparative analysis split the group into primary and secondary school respondents. As mentioned above, The i in online data set represents one of the largest ever detailed studies on the attitudes of primary school children toward privacy and data protection. In this section we explore their attitudes in more detail compared to their older counterparts.

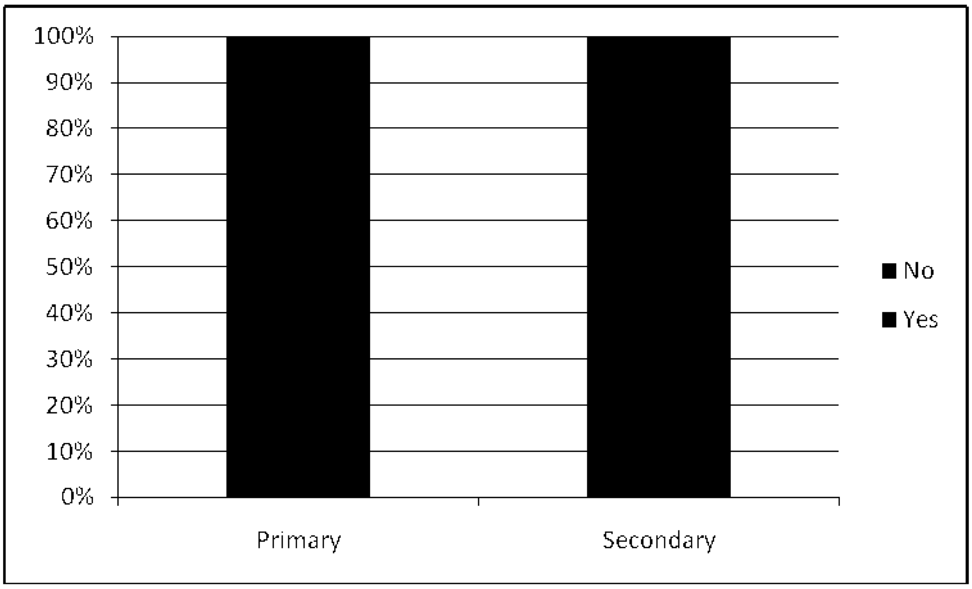

Figure 15 - Do you use social networks? Primary vs secondary

While it is unsurprising that more secondary aged respondents use social networks than primary school pupils, there is still a majority response of well over 60% which shows that many younger children are very much engaged in social networking and the privacy issues therein.

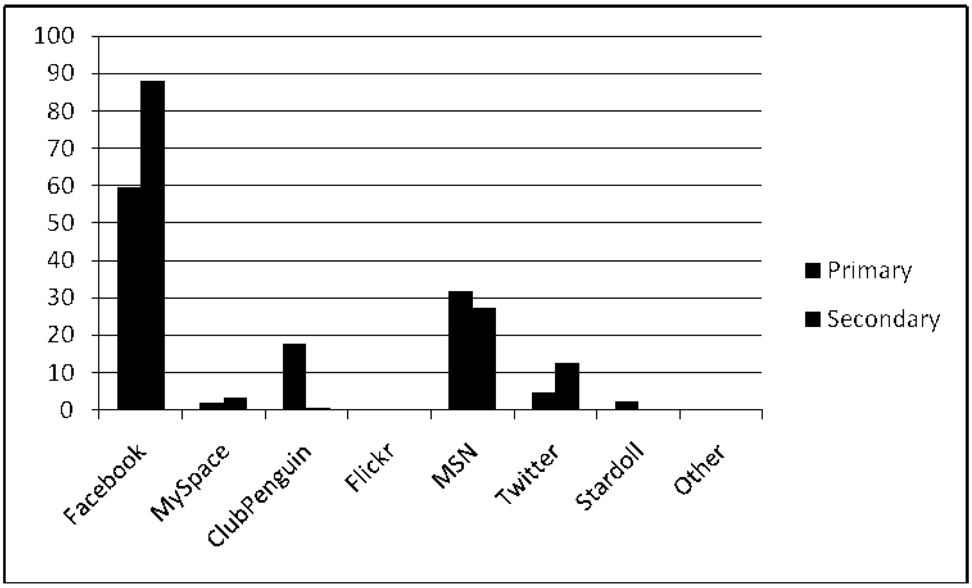

Figure 16 - Social networks used - primary vs secondary

For those who did use social networks, we have greater use (unsurprisingly) of Club Penguin by primary aged people, but it is very interesting to note that more primary aged pupils will use MSN than secondary school children. We are also looking at a population of primary school children very much engaged with Facebook, even though 13 is the “official” age limit for Facebook users. 60% of primary school children who use social networks will use Facebook. In total from our overall population 39% of primary aged children had used Facebook.

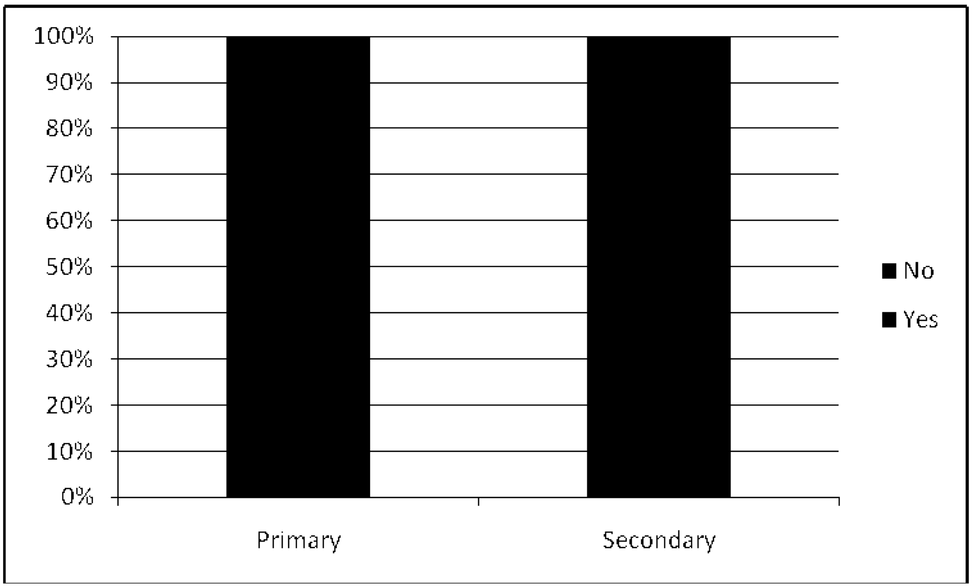

Figure 17 - Do you have an avatar - primary vs secondary

In terms of use of avatars, our results show that more primary aged children will use avatars than their older peers. While our data does not show much impact on the use of avatars in terms of attitudes toward privacy, it does highlight an interesting trend that younger children's behaviours do differ from their older counterparts. While conventional wisdom might suggest that younger children emulate their peers, our data suggest they are finding their own practices. This will have implications for the future (i.e. when these younger children become adolescent) as the behaviours of the younger children and attitudes will differ from their older peers.

Privacy Policies and Awareness

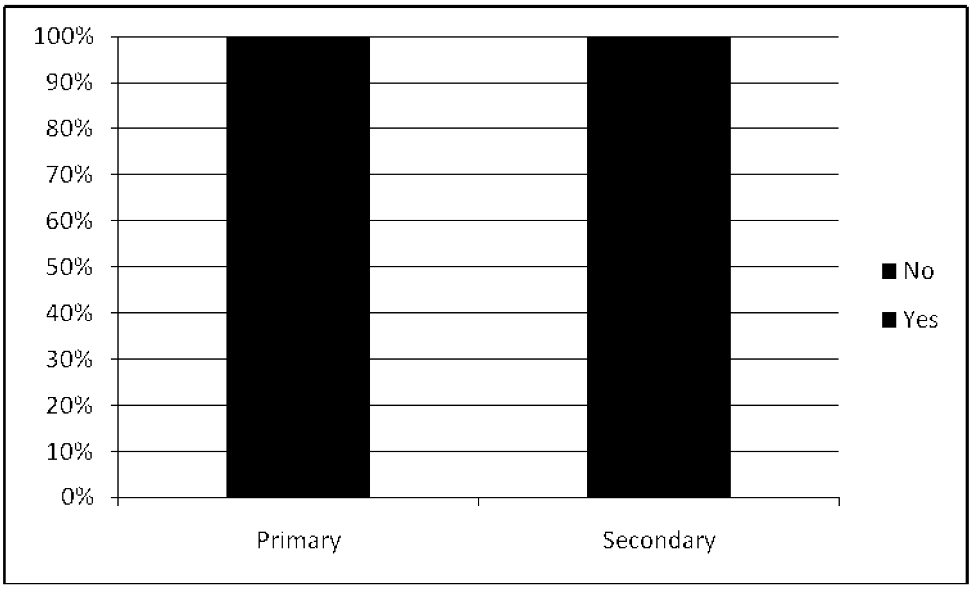

Figure 18 - Do you read privacy policies - primary vs secondary

In figure 18 it is clear that there is virtually no difference between the proportion of primary and secondary aged children who have read privacy policies. However, there are differences in terms of the reasons for both reading, and not reading, policies, explored in figures 19 and 20.

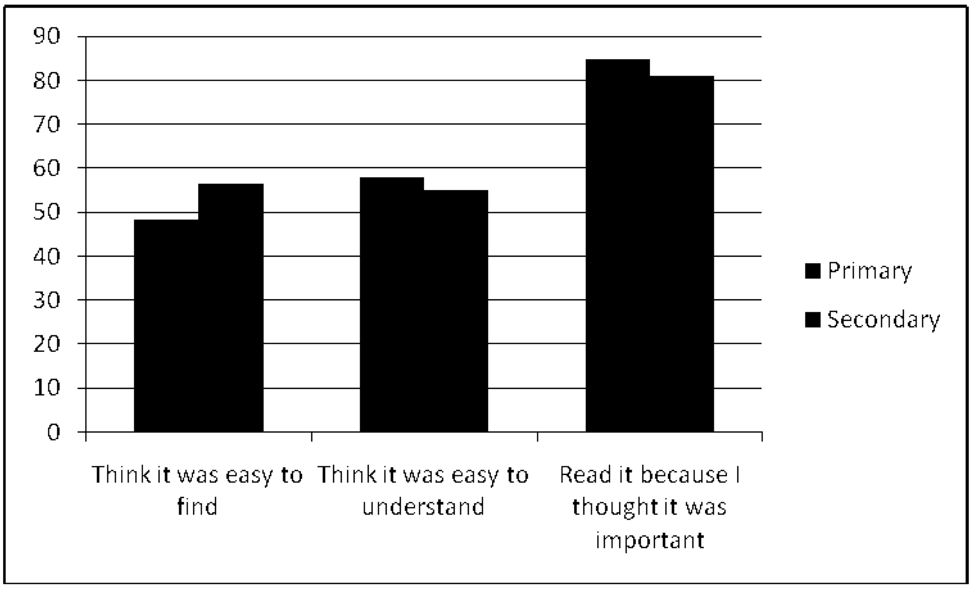

Figure 19 - If yes, did you...

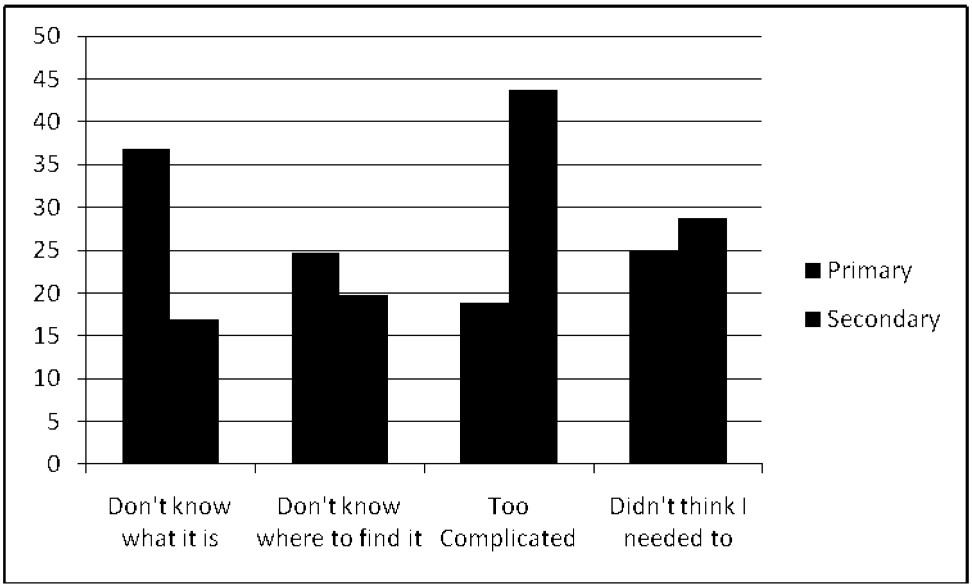

Figure 20 - If no, why not?

From these figures we can see that for those who have read privacy policies, primary school children are slightly less likely to think the policy was easy to find, but more likely to think it was straightforward to read, or read it because it was important.

The reasons for not reading policies are vastly different between the two sub populations. Primary school children are far less likely to be aware of what a privacy policy is (over a third of all primary school children in our population). Far less said they thought it was too complicated to read, but this might be because they either did not know what it was or couldn't find it.

Attitudes toward online privacy

In exploring the differences between primary and secondary aged pupils and their attitudes toward privacy, we consider the pattern of data sharing and also issues of consent once again.

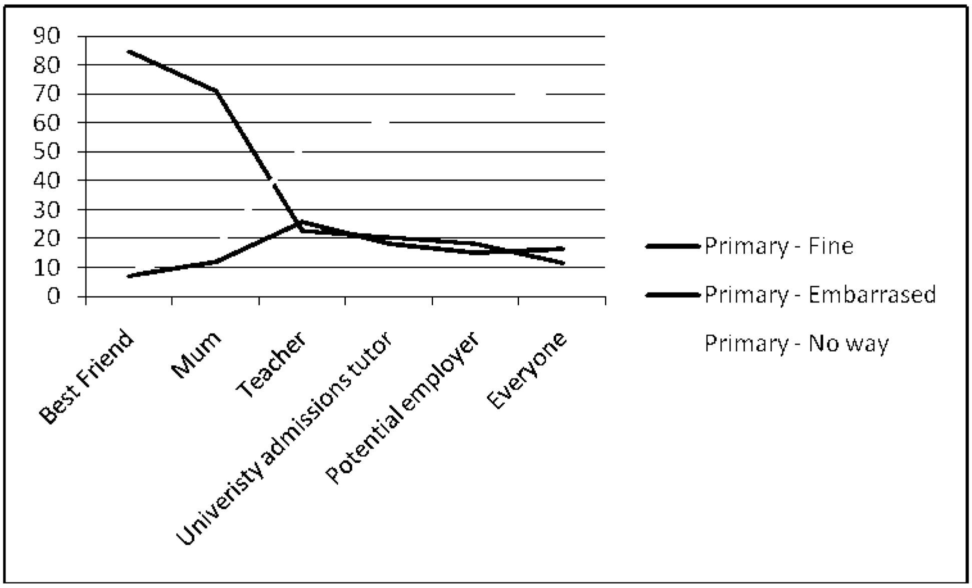

Figure 21 - - Attitude toward profile being seen, primary aged respondents

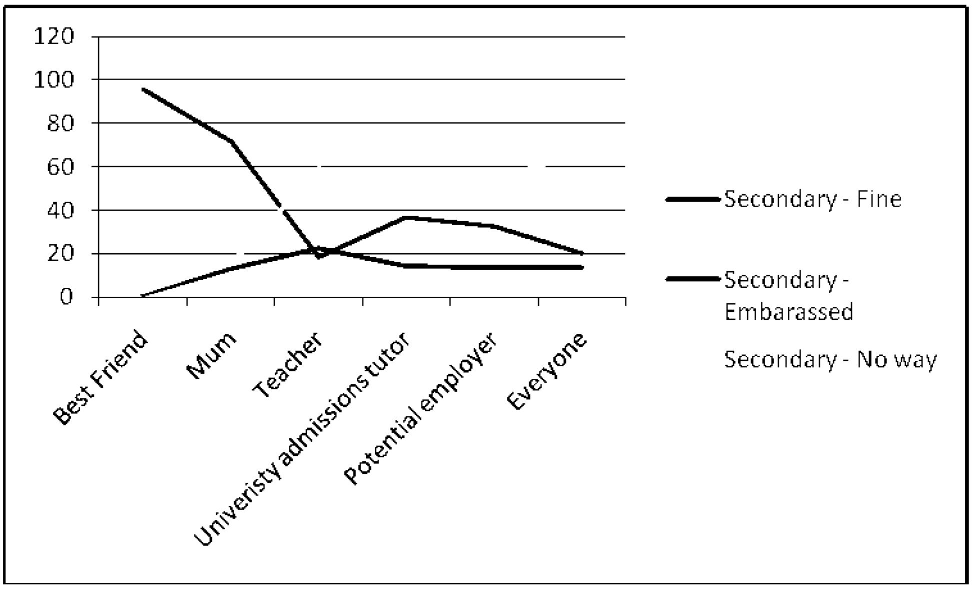

Figure 22 - Attitude toward profile being seen, secondary aged respondents

In figures 21 and 22 the difference in attitudes is clear to see. Primary aged pupils are very definite in that they would not be happy for anyone away from friends or family to see their profile. There is far less "no way" responses for secondary aged pupils and greater variation in who might see it and their attitudes toward such.

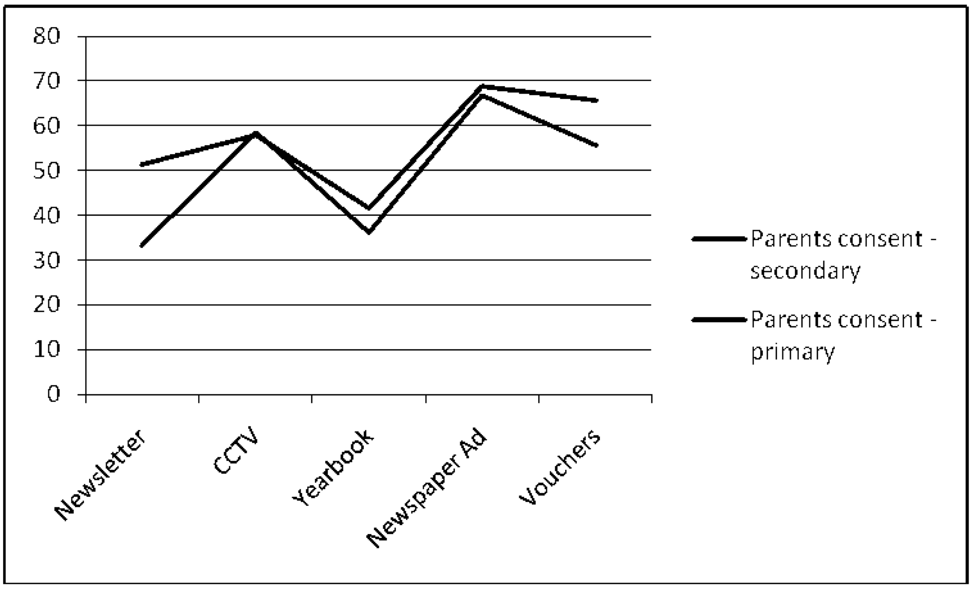

Figure 23 - Parental consent for a range of scenarios

Figure 23 returns to the issue of scenarios and the age of consent. Again a similar shape is shown for both sub populations, but we also have a difference between primary pupils, who are consistently more likely to say parental consent is needed for all scenarios.

In a final analysis, we will now move to focus on a specific group of primary users, those who use Facebook. This analysis holds a great deal of interest because it is rare to capture this amount of information about a population of under-aged Facebook users.

Primary Facebook Users

In total, 1128 respondents of primary age said they used Facebook. The most significant difference we can see in comparing Facebook primary users to the overall primary profile can be seen in figure 24. Facebook users are 10% more likely to have read a privacy policy than the overall primary population.

If we explore attitudes from those who had read policies, we can see that the Facebook users were more likely to know what a privacy policy was, and more likely to find a privacy policy complicated. This ties in with our earlier assumption that primary aged pupils do not think policies are complicated because they do not know what they are. Those who engage with them do find them complex in some instances.

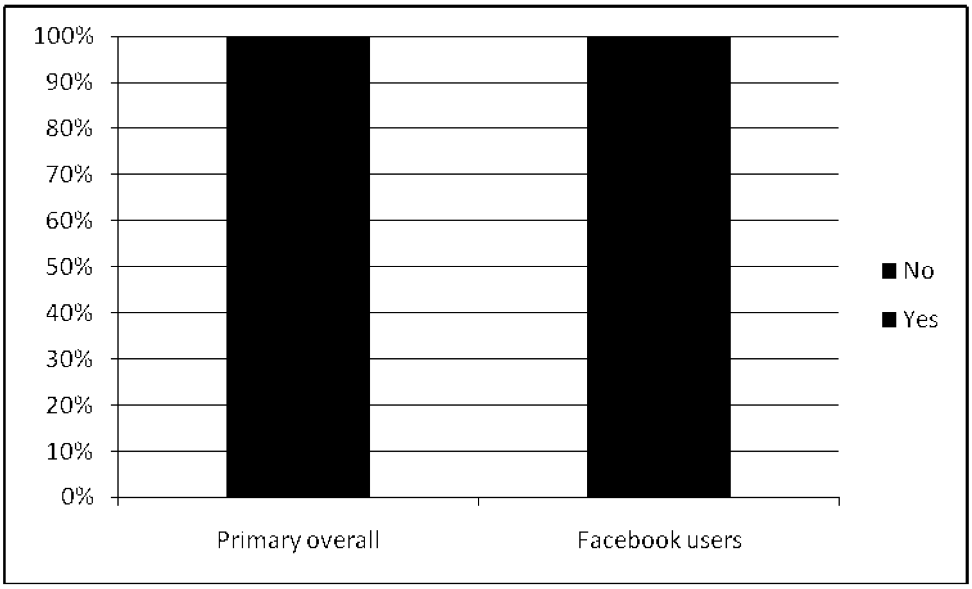

Figure 24 - Read privacy policy

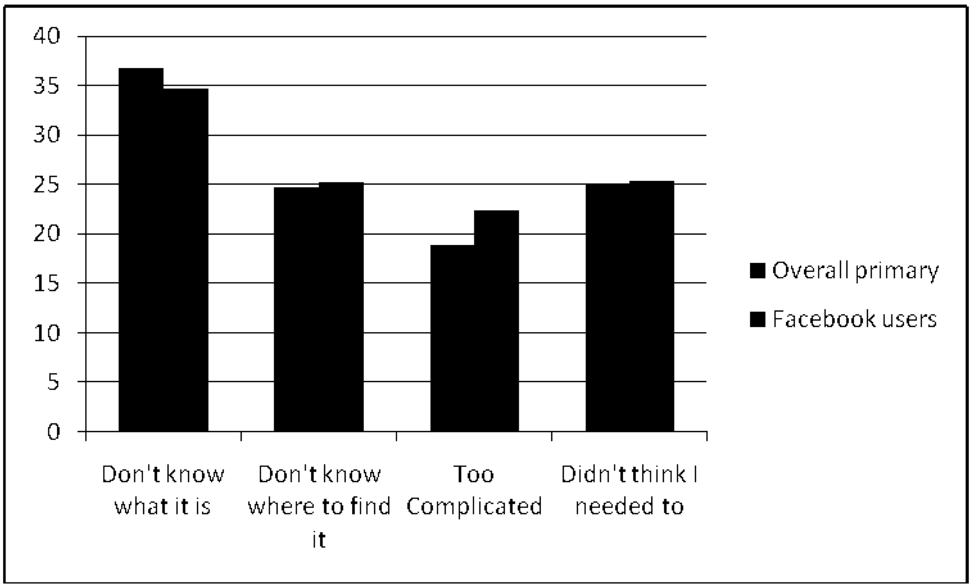

Figure 25 - If no, why not?

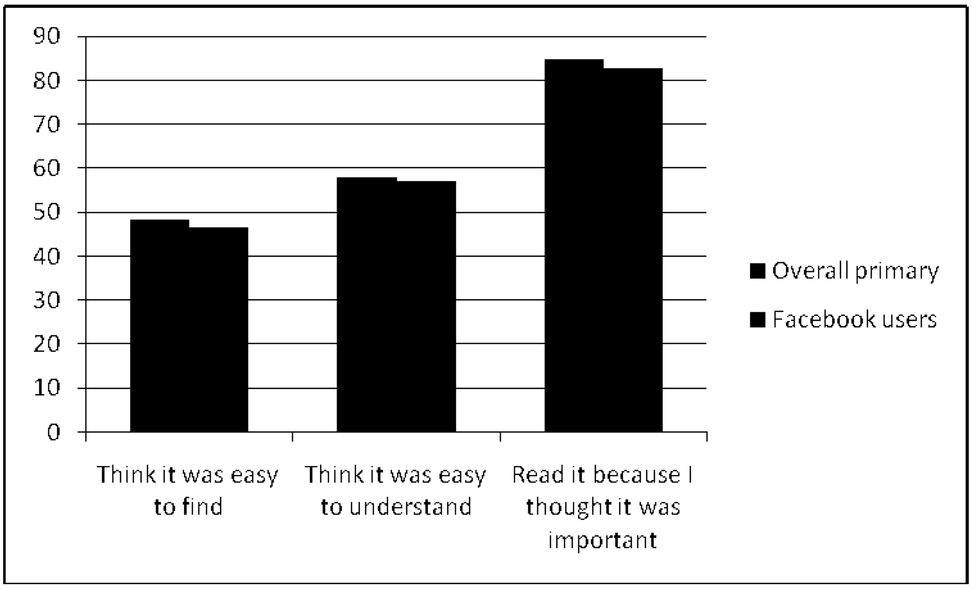

Figure 26 - If yes, did you...

However, as illustrated in figures 27 and 28, the Facebook users share similar beliefs in terms of who has their data. While there is slight variation in how they might feel for certain types of strangers saw their profiles, the variation is slight. This counteracts some of the more hysterical beliefs that social networks are responsible for children and young people becoming irresponsible with their data and with whom they share it. In fact, we can suggest from our data that those who engage in social networking practice are more responsible regarding privacy than those who do not.

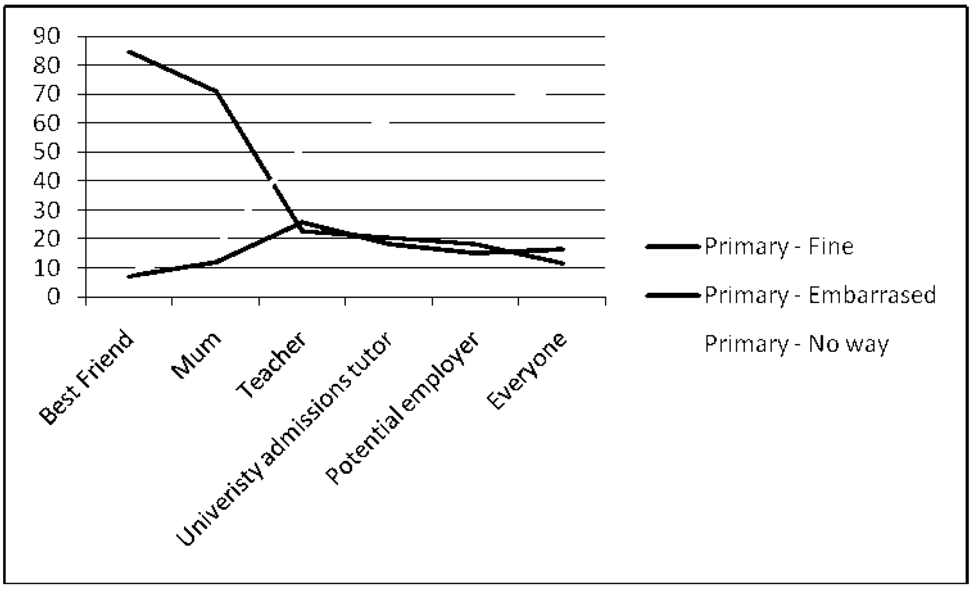

Figure 27 - Attitude toward profile being seen, primary aged respondents

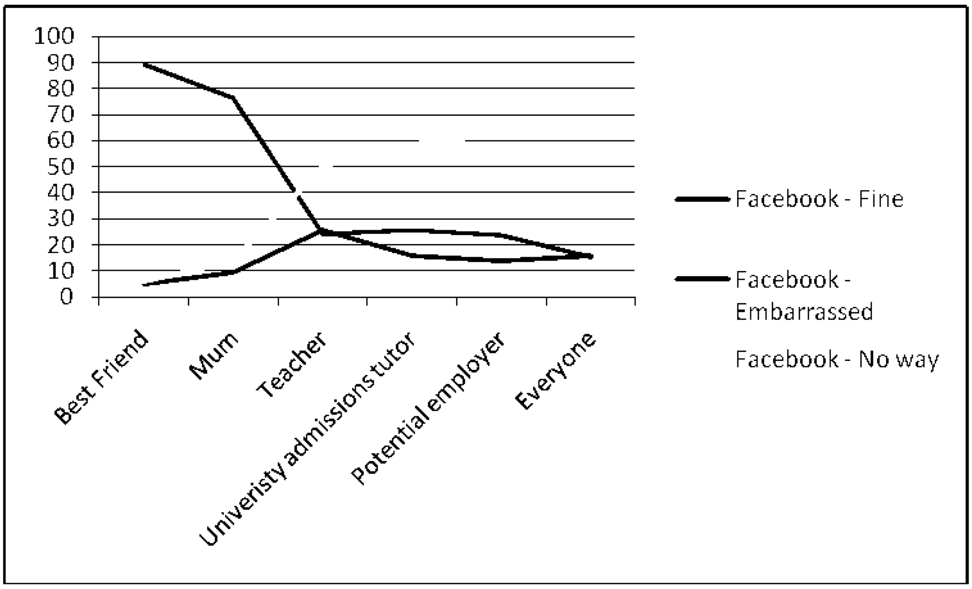

Figure 28 - Attitude toward profile being seen, primary aged respondents who are Facebook users

Acknowledgements

The i in online would like to thank the following people for their support with producing the Child Online Privacy Code and the Privacy Survey.

- Christopher Graham, The Information Commissioner
- Professor Andy Phippen, Plymouth University
- Caroline Bromley, Lamberhurst St Mary's Primary School
- Karen Jupp, St Edward's Secondary School
- Laura Gerrard, BPP Law School and their students
- Andrew Jeffcoat, BPP Law School
- David Rosenberg, Velorose

Section 2: About you

Are you:

A body representing the views or interests of children? Please specify:	☐
A body representing the views or interests of parents? Please specify:	☐
A child development expert? Please specify:	☐
A provider of ISS likely to be accessed by children? Please specify:	☐
A trade association representing ISS providers? Please specify:	☐
An ICO employee?	☐
Other? Please specify: Open Rights Group – a not for profit human rights organisation that focuses on the intersection of technology and rights.	☒

Thank you for responding to this call for evidence.

V1.0 20180626