Eyes Open Social Media Safety
Submission Queensland Parliament

Queensland Parliament Submission

Education, Tourism, Innovation and Small Business Committee

Inquiry into improving the delivery of respectful relationships and sex education relevant to the use of technology in Queensland State Schools

Eyes Open Social Media Safety Pty Ltd

ABN47 612 745 105

[redacted]

Ph: [redacted]

Submission prepared by Dan Munn – Research and Development Manager

Submission

Eyes Open Social Media Safety are a registered provider by the Office of the eSafety Commissioner and have been delivering social media safety and internet safety programs within Australian schools, predominantly in Queensland, since 2012.

Eyes Open Social Media Safety have educated over 30,000 students, teachers and parents on the dangers and risks of social media and internet safety. We also offer solutions to schools which educate students, teachers and parents on how to apply the most effective security settings to their personal social media accounts to significantly reduce the level of risk.

In each school we visit the majority of students are using social media, in fact most year 3 students are using social media in some form. On-line gaming is also considered social media use due to the ability of the games to freely allow for online interaction.

Social media is therefore a primary way in which students interact and with their friends and maintain relationships and often their digital relationships are viewed as important as their real word ones. Although we advocate for the positive use of social media this level of interaction and usage has its own inherent risks and dangers.

Through our research and extensive involvement within Queensland School communities we have identified 5 main risks and dangers associated with social media and internet use:

1. Inappropriate material, predominantly images and sexting – (Exposure to, distribution and procurement of)
2. Bullying
3. Identity theft
4. Predators
5. Digital footprints

From our experience we know that education must be presented in a very real way for students to relate to and identify with at least one of the risks and dangers. The best success has come from us researching the schools we visit beforehand and then showing students what we can find about their digital presence in public space. (We do not reveal their identity when this is presented). We also use real world stories, examples and actual cases so students can see for themselves, first-hand what is happening and what can go wrong.

From our extensive involvement within Queensland schools, and by using this method, we have found that nearly all students will relate to or identify with at least one of the risks and dangers presented. We also know that students do not want to be unsafe and when we use this method of teaching awareness is used, most students want to do something about it.

Our experience has shown that when a student follows our program and takes the steps necessary to better protect themselves against only one of the risks and dangers that they will actually protect themselves against all of the risks and dangers.

Our research has shown that there are only two solutions required to dramatically reduce the risk of harm and to promote a safe digital experience.

1. *Think before you post*
2. *Securing accounts*

Think before you post requires education and awareness about the risks and dangers (inappropriate material, bullying, identity theft, predators and digital footprints) and what makes students vulnerable to the dangers. The most effective way of delivering this is to conduct engaging age appropriate and content specific sessions within the school on an ongoing basis.

Think before you post is however not effective as a stand-alone solution. Why? Because students make mistakes and students inadvertently will put themselves at risk even the best awareness campaigns are in place.

Awareness only attempts to answer the "WHY" question, why you should or should not do something online and it does not answer the "HOW TO" question; how to become safer and what exactly needs to be done to make yourself safer online.

Given that students don't want to be unsafe online our experience shows that unless the "HOW TO" is taught correctly students often won't do anything about it.

Securing accounts is the key to ensuring students are best protected. Prevention is better than cure and having a safety net around students will help catch issues before they end up being out of control.

Social media sites by default are open, sites want maximum interaction and full public exposure. Security settings are often complex and convoluted and are not intuitive to navigate and set up. Students will often attempt to set up security on their accounts and end up getting it horribly wrong leading them to think they are secure when they are not and this is a very dangerous position for students to be in.

There is also a technical gap between what parents and teachers know about the social media sites used. Parents and teachers come from a place of wanting to help but often find they just don't know how to or they just "have a go" with the end result leaving students in the same position of thinking they are safe when they actually are not.

Eyes Open Social Media Safety have developed targeted age specific online courses which follow on from the awareness sessions which are designed to secure all the main social media sites that students use.

Our research has shown that when students are given a structured and easy to follow "hands on" course they will in fact make the changes necessary to make themselves safer. When this is run on the back of an awareness program they will also understand why they are making the changes.

One off awareness sessions do little to change behaviour. Sadly we have seen the norm to be Queensland schools just engaging in one off awareness sessions thinking that this is enough. We have the view that this is not enough. Programs need to be ongoing and not just about awareness, they need to give students the tools to make the changes to make themselves secure.

Parents and teachers also need to complete security setting courses to help bridge the technical gap and we have found that implementing a program which involves students, teachers and parents produces by far the best results. We have also found that leaving out one of these groups in the process reduces the effectiveness of the risk prevention.

Summary

Maintaining healthy and safe relationships in the digital world is just as important as maintaining them in the real world.

Awareness programs on the risks and dangers MUST be followed up with "how to" strategies. There is little point on providing education if the tools to make the changes are not also given.

Think before you post and *securing your accounts* are the two primary steps to reduce risk, improve prevention and to allow students to have a safer and more enjoyable time in the digital world.

Applying these rules to better protect a student from one of the five risks then better protects that same student from all the other risks and dangers on social media and in the digital world.

Recommendations

Schools need to adopt programs which incorporate the following:

1. Age specific targeted programs
2. Programs must be ongoing and imbedded into the school on a regular basis
3. Programs must cover awareness of the risks and dangers using real word examples which students can relate to or identify with
4. Awareness programs must be targeted to educate students to think before they post
5. Awareness "WHY" must be followed up with an action plan on "HOW" to improve safety online
6. Education on how to apply security settings to social media sites is critically important to improving prevention
7. Programs should involve students, teachers and parents

Please note that we are available to provide further information within this area and are also available to be involved in any discussions associated with this submission.

Regards

Dan Munn

Research and Development Manager