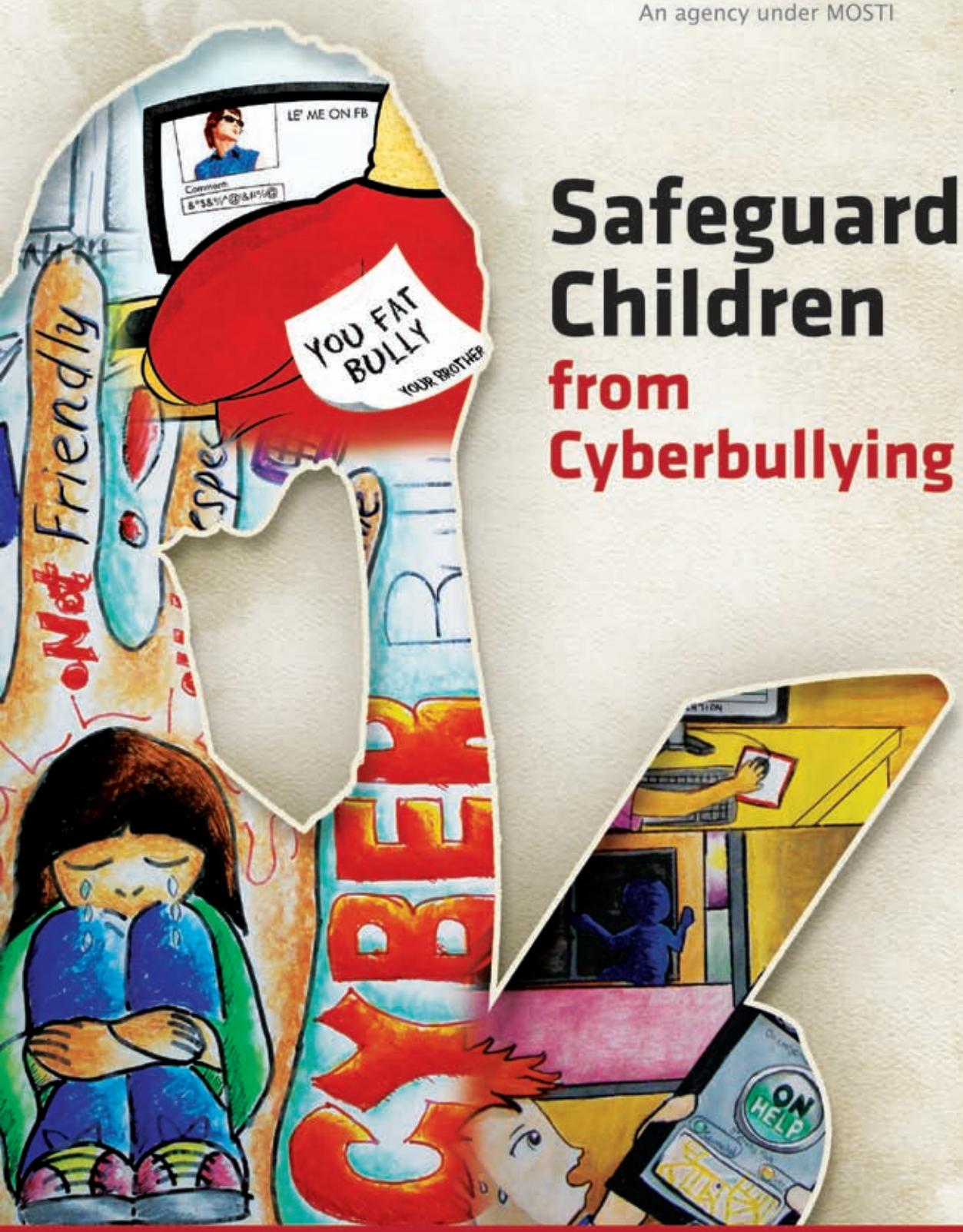
CyberSecurity MALAYSIA

An agency under MOSTI




# Safeguard Children from Cyberbullying

Securing Our Cyberspace

Registered office:
CyberSecurity Malaysia,
Level 5, Sapura@Mines,
No 7, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor, Malaysia

Phone: +603 - 8992 6888
Fax: +603 - 8992 6841
Web: http://www.cybersecurity.my

# Acknowledgement

CyberSecurity Malaysia wishes to thank the following individuals who have contributed and/or reviewed this guideline.

**External Contributors/Reviewers:**

1. Fatimah Zuraidah Salleh (Social Welfare Department)
2. Keith Woo (Persatuan Kebajikan Generasi Gemilang Kuala Lumpur & Selangor)
3. Professor Khaeruddin Sudharmin (Othman Yeop Abdullah Graduate School of Business, Universiti Utara Malaysia)
4. INSP Mohd Faizal Zainal (Commercial Crime Investigation Department, Royal Malaysian Police)
5. Navaneeswary Ganesamoorthy (Sirius Scholar Study Skills)
6. Nick Foong (Persatuan Kebajikan Generasi Gemilang Kuala Lumpur & Selangor)
7. Nina Mohamed Nor (Independent Creative Director/Brand Consultant)

**Internal Contributors/Reviewers:**

1. Aaron Mokhtar
2. Maslina Daud
3. Mohd Shamil Mohd Yusoff
4. Lt Col Mustaffa Ahmad (Retired)
5. Noor Azwa Azreen Abd. Aziz
6. Nurul 'Ain Zakariah
7. Sabariah Ahmad
8. Siti Hajar Mohamad Ali
9. Syafiqa Anneisa Abdullah (Author)
10. Zaihasrul Ariffin

# Table of Contents

# 1 What is Cyberbullying?

Technology has evolved tremendously. The Internet is accessible at any time and almost everywhere. The devices used to access the Internet are becoming more and more innovative and mobile. It has become a necessity and a way of life for many. School going children accessing the Internet and possessing mobile devices is not an unusual sight nowadays. This rapid advancement and evolvement of technology is a contributing factor to the change in the behaviour of children. Children can be seen interacting less physically, but instead, they are seen constantly interacting via social networking sites, playing online games, watching movies or even surfing the Internet whether at home or elsewhere.

There is a major rise in concern over the safety of children that are allowed access to the Internet due to the change of their behaviour. This is because the advancement of technology also comes with new and increasing number of threats. Without any parental control in place and without sufficient knowledge and awareness, it can jeopardize the safety of our children as they are known to be naïve and vulnerable.

Children are seen to be more bold and confident when they are online. They are bold to pass comments, post photos or videos because it is done online and not in person. This boldness and confidence are sometimes portrayed unconcealed and some are done anonymously. Because it can be done anonymously and they feel that their true identity is concealed, it augments their boldness. As a result of this, we see the emergence of a new form and medium of bullying. We are now faced with a bigger problem and on a larger scale. It is called Cyberbullying.

Cyberbullying is when a child[1] is distressed, humiliated or targeted using the Internet, interactive and digital technologies or mobile devices. Many people take cyberbullying very lightly. As a result, they are oblivious to the fact that their child is a victim of cyberbullying. Cyberbullying usually involves a string of communications or one time communication and may go to the extent of containing death threats or threats of bodily harm. Parents or teachers often take these hurtful, rude or embarrassing posts lightly without realizing the adverse effects it may have on a child and without realizing that it may drive a child to have suicidal thoughts and eventually, to commit suicide.

## 1.1 Forms Of Cyberbullying

These are methods of cyberbullying that a perpetrator can use:

a. Texting or emailing intimidating, rude or cruel messages to people e.g. “You are fat and ugly”, “You had better do what I ask or else....”
b. Posting or forwarding humiliating videos or photographs of someone on video-hosting sites or social networking sites e.g. indecent photographs or videos.
c. Distressing someone by sending repeated texts or instant messages in a chat room e.g. “I’m going to get you”.
d. Setting up fake profiles or using actual profiles on social networking sites to prank or make fun of someone.
e. Posting, forwarding or obtaining someone’s personal or private information without permission from the person.
f. Spreading rumours or lies about someone.
g. Happy slapping: where bullying or physical assaults are videoed and distributed.

[1] *Child Act 2001 defines a child as being a person under the age of 18 years.*

h. Flaming: online fights where scornful and offensive messages are posted on websites, forums, or blogs[2].
i. Outing and Trickery: Tricking someone into revealing secrets or embarrassing information, which is then shared online[3].
j. Exclusion: where a child is deliberately excluded from an online group[4].
k. Impersonation: where your child's email or other online accounts are hacked and messages that will cause embarrassment or damage to your child's reputation and affect his or her relationship with others.[5]

There are instances where children do certain things purely out of mischief or as practical jokes but with no malicious intent. However, they do not realize that anything that goes online can escalate and get out of hand very quickly and eventually cause an undesirable chain reaction.

## 1.2 Common Channels Used For Cyberbullying[6]

Based on a national survey conducted on school going children during the CyberSAFE in Schools Programme (2013), the outcome of the survey revealed that half of the students knew at least one person being bullied online and the following were the most common channels that were used for cyberbullying:

a. Facebook
b. Blogs
c. Short Message Systems (SMS)
d. Phone Call

---

[2] *http://internetsafety101.org/upload/Cyberbullying.pdf*
[3] *http://internetsafety101.org/upload/Cyberbullying.pdf*
[4] *http://internetsafety101.org/upload/Cyberbullying.pdf*
[5] *http://internetsafety101.org/upload/Cyberbullying.pdf*
[6] *A National Survey Report 2013 – Safety Net: Growing Awareness among Malaysian School Children on Staying Safe Online*

e. Hacking of online accounts
f. Videos, YouTube
g. Email
h. Videos, YouTube

Individuals or a group of people can perpetrate cyberbullying. The biggest distinction between cyberbullying and other types of bullying is that the cyberbully can follow you everywhere and at all times, into your house, even into your bedroom and the perpetrator can be someone you know or is anonymous. Another worrisome aspect of cyberbullying is that victims of cyberbullying often feel that there is nowhere to hide. They may not know whom they need to hide from and even if they do know the perpetrator, they may not know whom to turn to. Consequently, the victims live in constant fear or humiliation.

# Connect with RESPECT


*Designed by:*
*Muhammad Syahmi Bin Ghazali,*
*participant of the Poster Designing Challenge in conjunction with Safer Internet Day 2013.*

CyberSecurity MALAYSIA

MOSTI

SID 2013

# 2 How Do I Tell If My Child Is A Victim Of Cyberbullying

It is not possible to expect all children to behave in the same manner because each child has individual behavioural patterns. Many factors influence this e.g. upbringing, cultural background or surroundings.

These are examples of changes in a child's behaviour that serve as indicators of the possibility that a child is a victim of cyberbullying:

a. Observe for changes in your child's behaviour. Does your child look unusually and constantly upset or worried?

b. Observe for changes in your child's online behaviour. Is your child suddenly spending far more or far less time online?

c. Observe if your child becomes distressed after using the phone or computer. Does your child become troubled, annoyed, tensed or confused after going online or after a telephone call?

d. Does your child ask you out of the ordinary questions? For example, how to close down social networking site accounts, or about security features like blocking other account holders or phone numbers?

e. Has your child become more withdrawn? Not wanting to socialize much, not wanting to talk much?

f. Has your child reduced usual social activities, like going out and meeting friends? Going out daily at 5pm may be

routine. But all of a sudden, you notice that your child does not want to go out anymore at 5pm.

g. Has there been an increased tendency and frequency of illnesses or loss of appetite? Headaches, stomach upsets or other ailments?

h. Has your child's school attendance and performance deteriorated? Does your child hesitate or resent going to school? Pretends to be sick or comes up with reasons to avoid going to school?

i. Does your child act secretively when using the Internet or phone? For example, do they shut down the computer or hang-up suddenly when you or someone else walks past or enters the room?

j. Does your child look depressed or show signs of low self-esteem? For example, "I am such a hopeless kid", "I hate myself" or "Nobody likes me".

Regardless of the cause, a key rule of thumb to follow if you notice your child behaving in an unusual manner is to engage your child in conversation. Talking to your child will enable you to discover and understand the causes for your child's unusual behaviour. It will also fortify the bonding between you and your child.

# 3 Before You Allow Your Child Access To The Internet

A child should not be allowed access to the Internet without sufficient knowledge, awareness and guidance. These are measures that you may take before allowing your child access to the Internet:

***a.*** ***Be learned***. Educate your child on online safety practices before allowing your child to use gadgets or to surf the Internet.

***b.*** ***Be wise***. Install parental control softwares to filter unsuitable contents.

***c.*** ***Be open***. Computers should be placed in common or open areas.

***d.*** ***Be stingy.*** Impose rules and time limits for your child to access the Internet. This period of time should preferably be a period of time with as much supervision as possible.

# 4 When Your Child Is Allowed Access To The Internet

The following are measures which your child should adopt when they access the Internet:

***a.*** ***Be selective***. Constantly remind your child not to give out any personal details, such as phone numbers or addresses freely, especially to people that they do not know.

***b.*** ***Be cautious.*** Social media was created for people to socialize by sharing information, photos, personal details, exchanging views or to post happenings. Advise your child to share and post responsibly and wisely. Do not divulge too much information about themselves, their daily activities and whereabouts and they should refrain from chatting with strangers.

***c.*** ***Be sensible.*** Continuously remind them to be cautious when posting photos or videos of themselves, family or friends. Stress that indecent photos should never be posted and that they should never perform indecent acts on videos. Ensure that your child is aware and clearly understands that whatever posted online, will remain online forever and that the number of people who can view these posts are limitless.

***d.*** ***Be protective.*** Ensure that your child understands how important it is to protect their passwords, and never to give anyone access to their accounts. Advise your child to periodically change their passwords and to set passwords that contain a combination of numbers, alphabets and symbols. If your child does not know how to do so, teach them how to or do it with them or for them.

***e.*** ***Be wise.*** Most social networking sites have advice and guidance on safeguarding privacy. Ensure that your child customizes the privacy settings or do it for your child or with your child. Teach your child how to block instant messages or use mail filters to block unwanted or unknown emails.

***f.*** ***Be ethical***. Ensure and remind your child to always be polite when online. Online impoliteness can trigger a chain reaction. Always practice good netiquette when online.

***g.*** ***Be close.*** Always communicate and take interest in your child's activities and be alert of whatever your child tells or tries to tell you. Advise your 12 child to immediately inform you or anyone trustworthy if they are being bullied or if any action, person or anything is distressing them.

***h.*** ***Be kind.*** Advise your child to inform you if they know of anyone who is a bully or is being bullied and advise your child to never take part in any bullying.

# WHAT GOES AROUND COMES AROUND
# CONNECT WITH RESPECT


*Designed by:*
*Mohamad Jauhari Iskandar Bin Mat Jaafar*
*participant of the Poster Designing Challenge in conjunction with Safer Internet Day 2013.*

# 5 What Should I Do If My Child Is Being Cyberbullied?

Most of a child's time is spent either at home or at school. As such, parents, siblings or relatives should play a bigger role in ensuring a child's online safety, followed by teachers. Parents and teachers may play similar roles but the distinction between the roles would be, different levels of authority and in different environments i.e. at home and in school. Nevertheless, either way, parents and teachers can collectively contribute significantly to minimizing the risk of children being victims.

## 5.1 My Child Is A Victim

When you discover that your child is a victim of cyberbullying:

a) DO NOT ignore it
b) DO NOT panic
c) DO NOT overreact

## 5.2 What Should I Do?

Address the situation calmly and cautiously. Do not react in a manner which will cause your child to retract and withhold important details of what happened.

***a. Have a clear understanding of the situation***. Calmly ask your child to tell you what exactly happened or has been happening. A clear understanding of the whole situation will enable you to gauge the severity of the situation.

***b. View the evidence***. Ask your child to show you the email, message or post. Collect as much information as possible.

c. ***Explain to your child.*** Once you have identified that your child is a victim of cyberbullying, explain to your child what cyberbullying is. Help your child understand that he/she is a victim of cyberbullying and that what the perpetrator is doing is not right and it must stop.

d. ***Reassure your child.*** Comfort your child by reassuring your child that you will always be there for him/her and that you will resolve the problem together. Emphasis must be given to ensure that your child understands that what the perpetrator is doing, is wrong.

e. ***Do not respond or comment***. Tell your child never to respond to malicious, intimidating or provocative emails, messages or posts, because responding or reacting would only mean that the cyberbully has achieved the goal in humiliating or intimidating your child. A response or reaction may make things worse.

f. ***Do not delete.*** Do not delete the emails, messages or posts. They should be saved and kept as evidence, to aid in tracing the perpetrator. Although anonymous, the perpetrator can still be traced, as they would leave cyber footprints.

g. ***Lodge a report***. If your child receives online physical or sexual threats, immediately lodge a police report. If the incident involves your child's schoolmate, bring the matter up with the school's counsellor or principal.

h. ***Seek help.*** If you find that your child is extremely distressed, you should seek professional help.

# 6 How To Avoid Being Cyberbullied?

It is not easy to keep abreast with the rapid advancement of technology. In this current era, the need to be Internet or social networking savvy is inevitable. We do not want to be left out in conversations or left behind in terms of technological advancement. More importantly, it is a necessity to possess some knowledge on information security, online safety measures and to be aware of existing threats that are lurking, as we need to provide our children with guidance and education to ensure that our children enjoy a safer online presence.

Explain clearly and ensure that your child understands the repercussions of certain actions as they may not be aware or realize the effects of those actions. These online safety measures and repercussions of actions should be updated as and when required and repeated as many times as necessary. It is also vital to foster constant and open communication with your child. By doing so, it increases the confidence and likelihood of your child turning to you for assistance if he/she is faced with a problem. Always take interest in whatever your child tells you regardless of how trivial or ridiculous it may seem to you. Look out for unusual stories, questions, comments or behaviour as these may be tell tale signs or indirect signals of distress.

A child may be able to avoid being cyberbullied if he/she possesses sufficient knowledge of online safety, constantly reminded of the Do's & Don'ts and if they use the Internet and electronic devices cautiously and wisely. Do monitor your child's Internet activity closely and ensure that you play a vital role in your child's life and get involved in your child's activities.


*Designed by:*
*Mimi Amirah Bt Abdul Aziz participant of the Poster Designing Challenge in conjunction with Safer Internet Day 2013.*

# 7 Supportive Roles A Teacher Can Play at School

Children spend a substantial amount of time in school. As such, teachers can play an equally important role as parents and relatives, in mitigating risks of pupils becoming victims of cyberbullying. Some children may feel more comfortable to confide in their teachers as opposed to their parents as they may be afraid or may be uncertain of their parent's reaction.

The following are measures that a teacher may take:

a. Learn about online safety measures and lurking threats and impart that knowledge to the pupils.

b. Instil and constantly remind the pupils about the importance of being ethical whether offline or online and to say or post things with caution.

c. Encourage and advise pupils to come forward if they are being bullied, or if they have knowledge of anyone being a bully.

d. Advise pupils to refrain from taking part in any bullying by not passing comments, videos or photos around.

e. Interact with pupils on social networking sites e.g. Facebook. Teachers may set up a dedicated profile specifically for this purpose. This will provide a teacher with a wider platform to supervise and provide guidance to pupils. This will also enable a teacher to observe for unusual behaviours of pupils.

f. Conduct Internet safety campaigns or organize security awareness programs to educate and increase the awareness of pupils. This can be carried out by the school or by engaging a third party.

g. Do not take complaints from pupils lightly. Take necessary actions immediately.

Education, awareness and communication are vital components to ensure that our children do not fall prey to lurking threats. The repercussions will vary and can result in long term and adverse outcomes, which can mar the bright future of a child or hinder the development of our children. These outcomes can be avoided and it does not require a large amount of effort.


*Designed by:*
*Siong Chye Soon participant of the Poster Designing Challenge in conjunction with Safer Internet Day 2013.*

# 8 References


1. Laws of Malaysia, Act 611, Child Act 2001, published by The Commissioner of Law Revision, Malaysia under the authority of the Revision of Laws Act 1968, http://www.agc.gov.my/Akta/Vol. 13/Act 611.pdf retrieved on 20th February 2013
2. Covenant Eyes, http://www.covenanteyes.com/resources retrieved on 20th February 2013.
3. Kids Help Phone, *http://org.kidshelpphone.ca/media/80712/2012-cir-cyberbullying.pdf* retrieved on 27th February 2013.
4. Internet Safety 101 *http://internetsafety101.org/upload/Cyberbullying.pdf* retrieved on 3rd June 2013.
5. Hinduja, Sameer & Patchin, Justin W, Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying. Thousand Oaks, California, Corwin Press, 2009
6. Shariff, Shaheen, Cyber-bullying: Issues and Solutions for the school, the classroom and the home, London; New York: Routledge, 2008
7. Limber, Susan P, Kowalksi, Robin P & Agatston, Patricia W, Cyber Bullying: A Prevention Curriculum for Grades 3-5. Center City, MN: Hazelden Foundation 2009
8. Limber, Susan P, Kowalksi, Robin P & Agatston, Patricia W, Cyber Bullying: A Prevention Curriculum for Grades 6-12. Center City, MN: Hazelden Foundation 2008
9. Willard, Nancy E, Cyberbullying and Cyberthreats: Responding to The Challenge of Online Social Aggression, Threats and Distress. Champaign, Ill.: Research Press, c2007
10. A National Survey Report 2013 – Safety Net: Growing Awareness among Malaysian School Children on Staying Safe Online.

*Corporate Office:*
**CyberSecurity Malaysia**
Level 5, Sapura@Mines
No 7, Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia

Tel : +603 8992 6888
Fax : +603 8992 6841
Email : info@cybersecurity.my
Customer Service Hotline : 1300-88-2999
**www.cybersecurity.my**