GOLDEN POPPY INC., ONLINE SAFETY GUIDELINES

Last Update: May 13, 2019

Being online can be fun, sociable and inspiring. At Golden Poppy Inc., (GP) we want you to enjoy the time you spend online at our sites and using our products and services. For that reason, we've prepared a few tips to help you stay safe when online.

It is important that when you chat, use instant messenger (IM), or participate in other forums, you keep the following things in mind:

1. Talk to your parent or guardian so that they can set up rules for going online such as the time of day, length of time and appropriate areas for you to visit.

2. Never share your password or password hints with anyone.

3. Follow the rules of Internet sites, including those rules that are based on age of use, parental approval and knowledge, and public laws.

4. Tell an adult right away if you come across or receive any information that makes you feel uncomfortable.

5. Do not share private or very personal information. Never post or send anything that can be used to locate you or another person offline, such as a full name, email or home address or phone number.

6. Do not give out your parent's or guardians' work address/telephone number(s), or the name and location of your school without the permission of my parent or guardian.

7. Never send a person a picture of yourself or anything else without first checking with your parent or guardian.

8. Never agree to get together with someone you "meet" online without first checking with your parents or guardians. Have your parent or guardian set up the meet in a public place.

9. Don't take on bullies or cyber-bully anyone else. If someone taunts you, walk away from the computer. Report the person or behavior to an adult.

10. If something sounds too good to be true, it probably is. Check to see if it is a hoax and do some fact checking if you aren't sure about something.

11. Do not open, respond to or forward an email or instant message unless you know the person who sent it to you and you've checked it for viruses. The content could contain damaging software (such as spyware or viruses) or it might be offensive.

12. Use security software (such as virus scanners) to ensure your system is up-to-date and protected in case an email from someone unintentionally infects your computer.