CMSGu2012-01

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Windows 7 Parental Controls

CERT-MU

National Computer Board
Mauritius

Version 1.0

January 2012

Issue No. 1

Table of Contents

Figures

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

This guideline is for the most part aimed at assisting adults in protecting children's online interactions and activities.

1.2 Audience

The target audience for this document includes parents, teachers, rectors and the public in general, who can help children be safer and more secure on the Internet.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a background on online issues and parental controls.

Section 3 describes how to set up parental controls in Windows 7.

Section 4 discusses additional rules to protect children's privacy and safety on the Internet

Section 5 concludes the document.

Section 6 comprises a list of references that have been used in this document.

Appendix A defines a set of acronyms used in this document.

2.0 Background

The Internet has grown quickly in recent years, adding unimaginable services that enrich our children's lives. Unfortunately, these new technologies have also brought lots of concerns, for example, sexting, cyberbullying, Internet pornography and online predators, for parents. Fortunately, technology has also provided parents with some help, that is, parental controls.

2.1 What are the issues?

Cyberbullying

The National Crime Prevention Council's definition of cyber-bullying is "when the Internet, cell phones or other devices are used to send or post text or images intended to hurt or embarrass another person." Cyberbullying is increasingly recognized as a growing problem among tweens and teens.

Sexting

Sexting is a practice among teens of sending sexually explicit messages and photographs over the Internet, particularly with mobile phone cameras. Sexting can humiliate victims, and when the subject of the photograph is a minor, it is a crime.

Privacy

Children and teens sometimes fail to understand the ease with which personal information can be public on the Internet. A child's name, address, phone number and other personal information should not be shared with companies, marketers, and adult contacts.

Predators

Children who communicate online may come into contact with adults, some of whom may be sexual predators. Parents can help prepare their children for this possibility by taking some appropriate precautions.

2.2 What are parental controls?

Parental controls are tools embedded in computers and other electronic devices that allow parents to set limits for their children on how these products are used. Parental controls can help shield children from unwanted contact, restrict their access to inappropriate material, inform you of troublesome online behavior, and help to prevent the sharing of private information.

It would have been very helpful if parents could simply purchase a set of "controls" that would instruct children in online safety and screen out dangers. However, no piece of software can do all of this, parental controls combined with online safety education and some common sense rules for Internet use are a parent's best strategy for keeping children safe online.

Parents must always keep in mind that parental controls are tools, and are not a substitute for parental involvement and safety education. Parental controls provide one or more of five main functions: content filtering; use restrictions; contact management; privacy protections; and monitoring. Below is a brief overview of each area:

- **Content Filtering**

  Content restrictions are most often included in Internet parental controls, especially the ability to limit specific types of web sites deemed inappropriate for children. Content filtering is also included in gaming consoles to restrict access to mature video games, as well as media players to restrict access to music with explicit lyrics.

- **Use Restrictions**

  Use restrictions are limits on which features or programs of a device a child can use. Internet use restrictions can include blocking applications like e-mail or instant messaging. Gaming consoles and mobile phones can limit functions like Internet access or the ability to purchase items online, or block the ability to use functions like a camera. Use restrictions also include time management functions that allow parents to limit the times a child is allowed to use a device.

- **Contact Management**

  Contact management functions allow parents to control who can contact a child through communication methods such mobile phones, e-mail, instant messaging, or social networks. Contact management usually involves the parent managing a "white list" of approved e-mail addresses or phone numbers that are allowed to contact the child. Many contact management functions also include "black lists" where the parent or child can "black list" a phone number or e-mail address so it can no longer contact the child.

- **Privacy Protections**

  Content filtering and contact management focus on blocking *incoming* information, privacy protections focus on blocking *outgoing* information. Privacy protections include the ability to block the release of information the parent has deemed private, such as home address or phone number, or GPS data from a mobile phone that reveals location.

- **Monitoring**

  Monitoring enables the parent to record information about the child's activities online. Monitoring functions can include recording website visits, mobile phone call logs, e-mail exchanges or instant messaging transcripts, and even complete "screen capture" recordings that detail every activity online.

3.0 Setting Up Parental Controls in Windows 7

With all the shocking stories we hear about children meeting people online who are usually not who they say they are, and kids getting exposed to inappropriate content when they use the Internet, it is important for us to be aware that we can restrict and record what children do when they are online.

In Windows 7, you can set limits on your kids' computer us and help them be safer online without having to constantly peek over their shoulders to know what they are doing on the Internet. Parental Controls help you limit how much computer time children have, as well as which programs and games they can use and when they can do so. With the Parental Controls in Windows Media Center, you can also block access to offensive TV shows and movies.

Windows 7 allows you to control how and when your children use the computer. With the built-in parental controls, you can control:

- The times and days in which they can use the computer
- What programs they can run
- What games they can play

By also using **Windows Live Family Safety Filter**, you can also:

- Block inappropriate web sites from the Internet
- View logs of your children's activity both online and with general computer use
- Keep track of your child's online contacts and approve/deny requests

To install the **Family Safety** features, you must install **Windows Live Essentials**, via **Windows Update** (press **Start** and type in '**Windows Update**', then follow the on-screen prompts).

3.1 Enabling Parental Controls

To enable parental controls, press **Start** > **Control Panel**. Then, under **User Accounts and Family Safety**, click on **Set up parental controls for any user**:

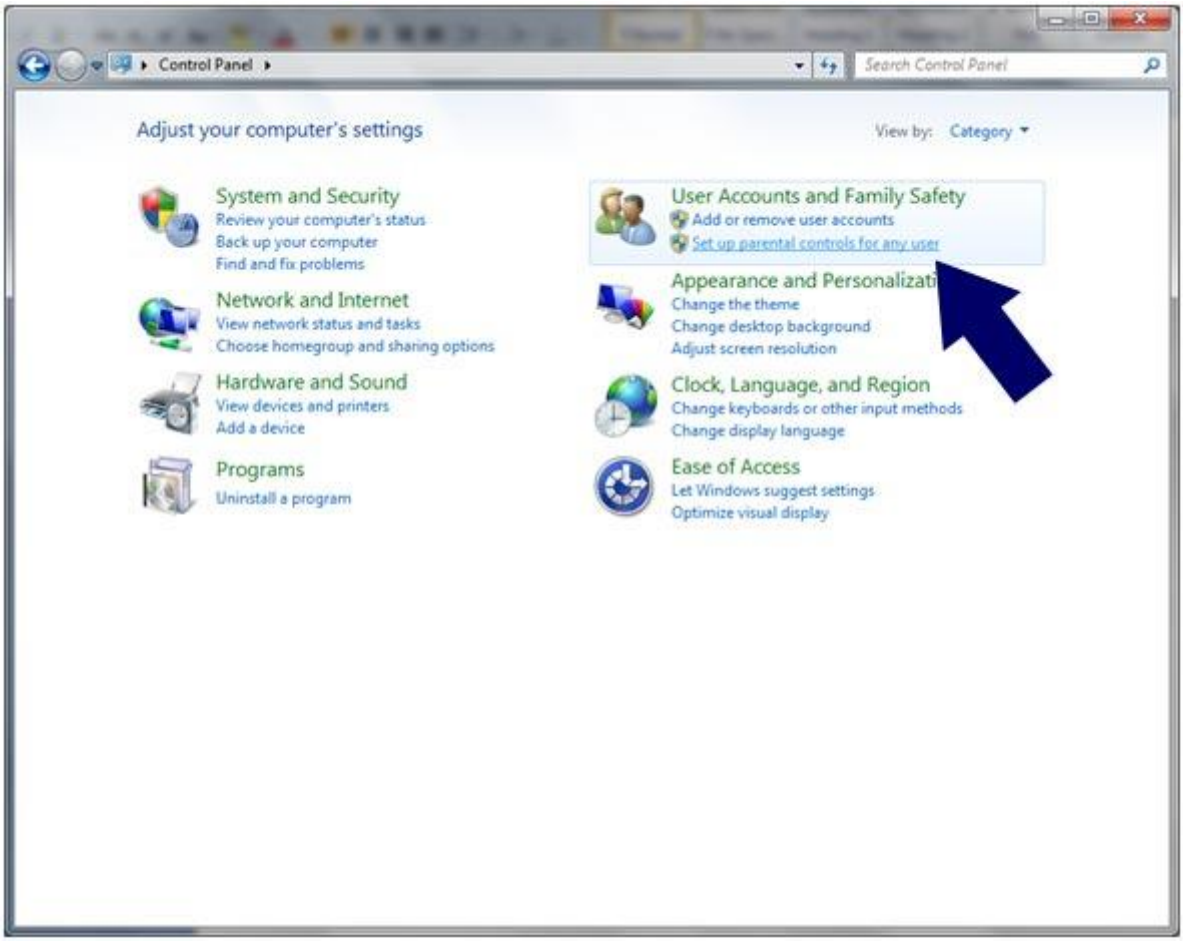

Figure 1 User Accounts and Family Safety

The next screen will show you all user accounts on the computer, so that you can apply Parental Controls individually to each child's account:

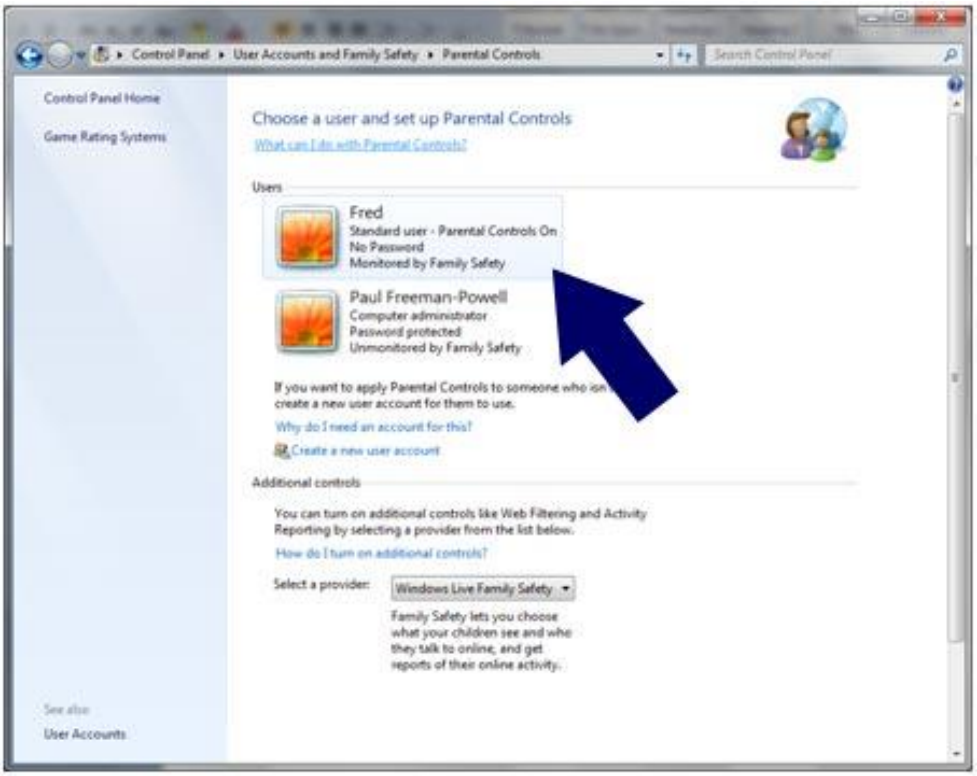

Figure 2 Choose user and set up Parental Control

Clicking on the account that you wish to control will bring up the following screen:

Figure 3 New user settings with Parental Control

Make sure the top setting is set to **On**, and then you may configure the restrictions.

3.2 Limiting When Your Children Can Use The Computer Using Time Limits

To control when your children may use the computer, click on the ***Time Limits*** section then simply click and drag to select and deselect time limits for the user's account:

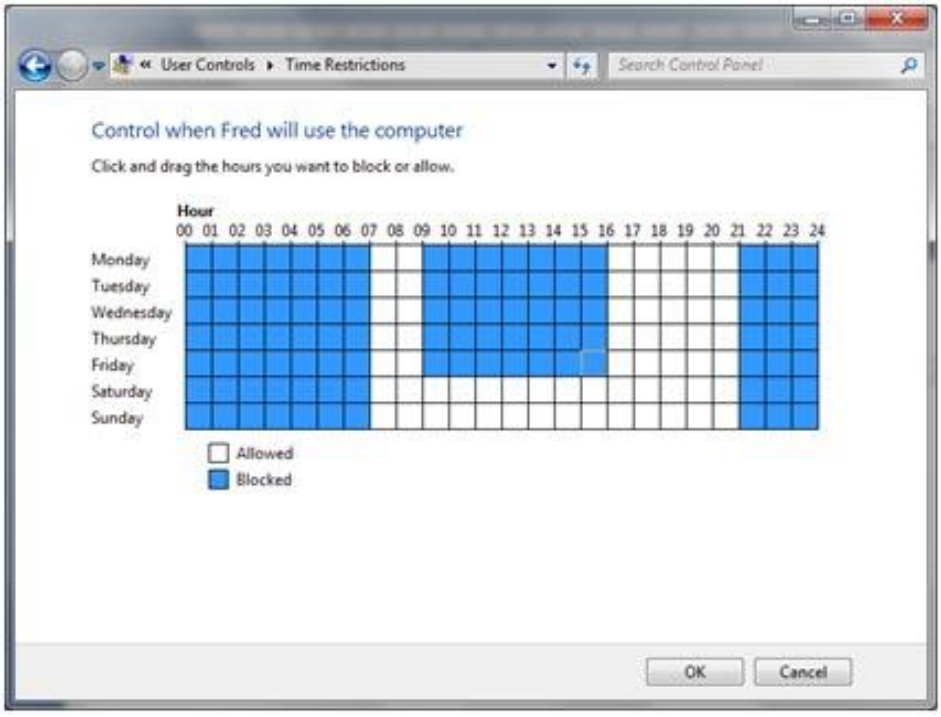

Figure 4 Control when your kid will use the computer

The example to the left shows a setup where the computer is always off-limits after 9pm and until 7am each morning.

The computer is also off-limits during school hours, but is free all day at weekends.

Adjust the limits to suit your own personal schedule.

3.3 Limiting When or If Your Children Can Use The Computer to Play Games

You can ban games altogether, for example if your child has access to two computers and one has been set aside as solely for school work.

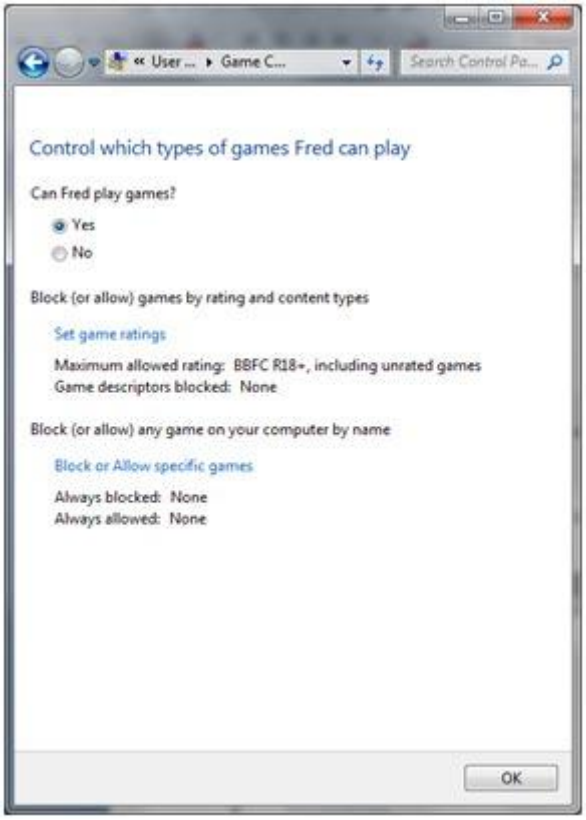

Figure 5 Control which types of games your kid can play

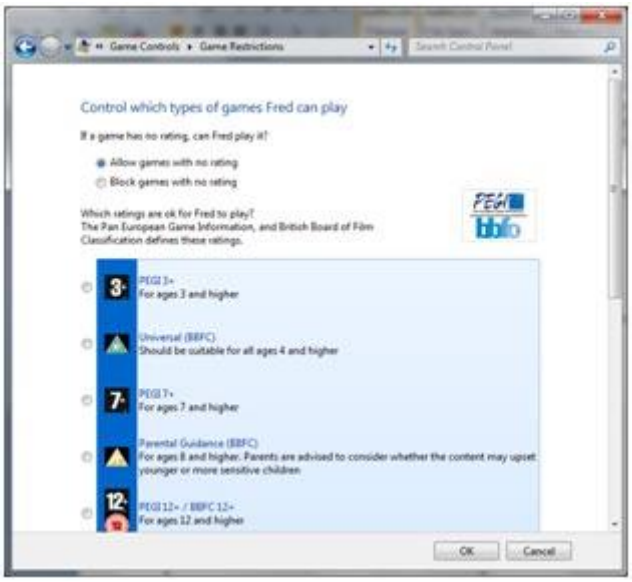

Figure 6 List of games allowed after Parental Controls have been set

Otherwise, press the **Set game ratings** link to set the maximum rating that the account's settings will allow.

You may also block other types of potentially objectionable content, and this setting will override any rating (see box on left).

You can also block or allow specific games, regardless of their content or rating.
To do this, simply press the **Block or Allow specific games** link on the main **Game Controls** screen.

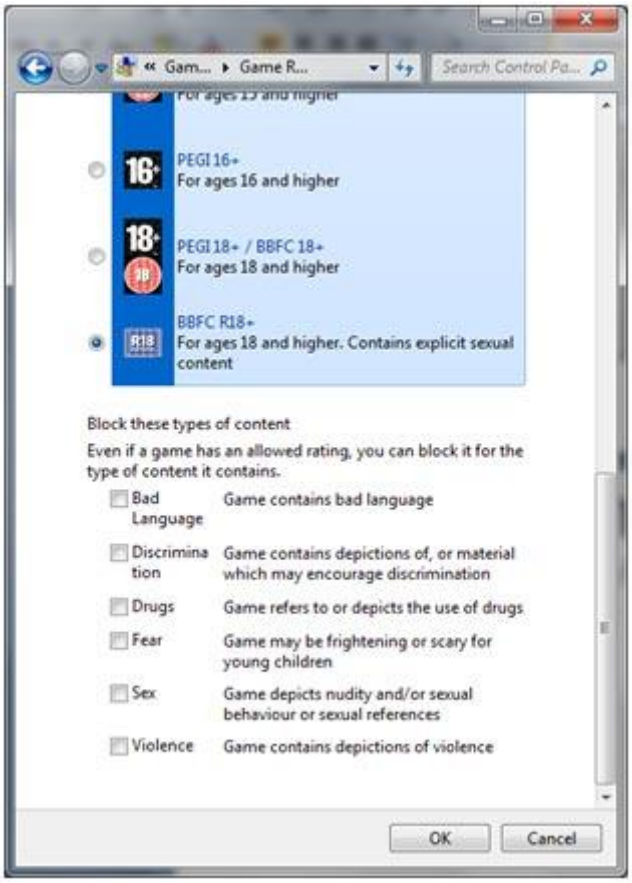

Figure 7 Games Controls

3.4 Blocking Access To Certain Programs

You may also wish to block access to certain programs which are installed on your computer. For example, you may have software installed for your own account to use but not want your children to use the software. To configure this, select the **Allow and block specific programs** option:

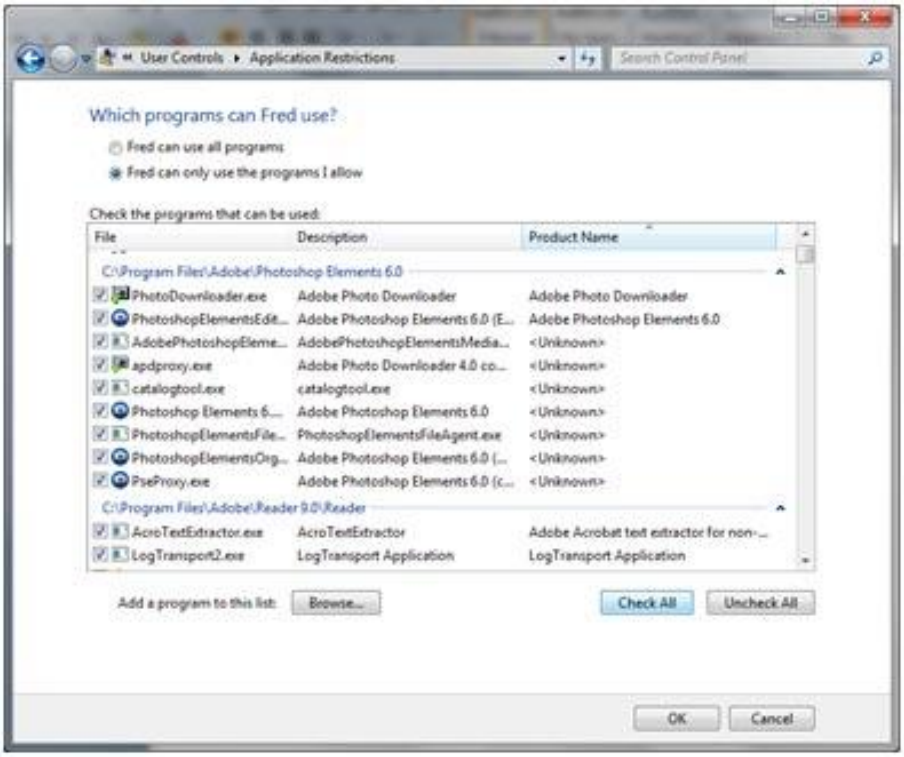

Figure 8 Application Restrictions

Tip: to allow access to most programs, first press the **Check All** button, then scroll through the list unselecting any programs to which you wish to restrict access.

3.5 Restricting and Monitoring Your Child's Internet Usage

The **Additional Controls** allow you to control how your child uses the internet, and prevent them from getting themselves into potentially undesirable situations, as well as protecting them from unsuitable content.

Figure 9 Additional Controls

Select the provider from the list. In this guide, we use Microsoft's own system, **Windows Live Family Safety**. If this is not already installed as part of **Windows Live Essentials**, you will be prompted to install the program or you may install it through Windows Update.

Once you have installed the suite, you may need to restart your computer. You must have a Windows Live ID (account) in order to proceed. If you do not have an account, you may create a free account and choose a password that your children will not know!

Note: once you have selected **Windows Live Family Safety** as a provider, it will take over control of the basic settings too, meaning they are all configured in the web browser. This means that you can control these settings from any computer in the world that you are logged into with Windows Live.

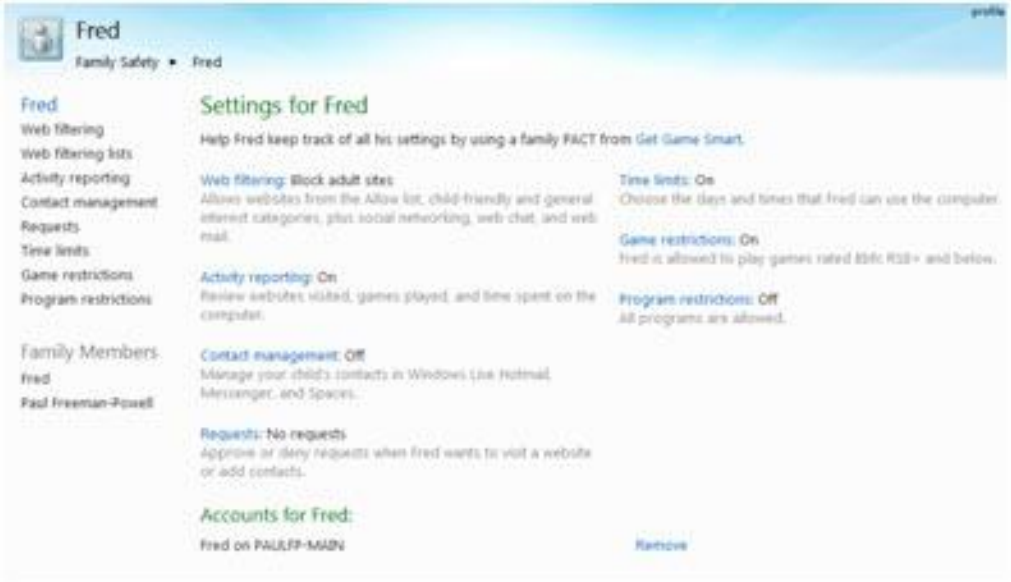

Figure 10 Windows Live Family Safety

Press the account you wish to control, then the configuration pages will load in your web browser (**left**).

This allows you to control all settings from the same screen.

3.6 Set Up Web Filtering On Your Child's User Account

To set up web filtering for the account, press the Web filtering link and choose the appropriate level of filtering for each account.

Figure 11 Web Filtering

To block or allow specific web sites, press the **Web filtering lists** button on the left-hand menu:

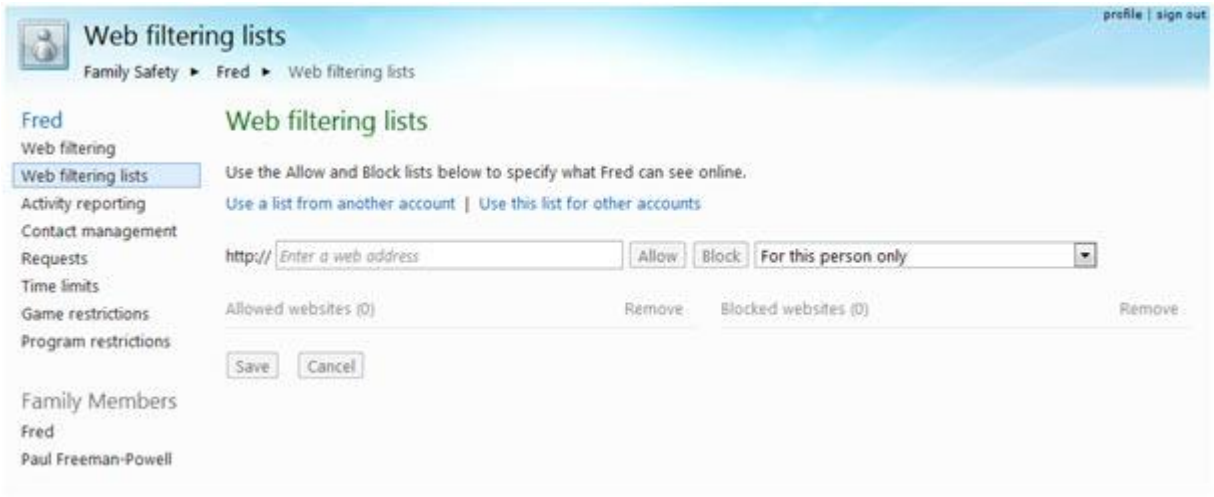

Figure 12 Web Filtering Lists

If your child attempts to view a web site which has either been specifically blocked, or has been blocked automatically due to its content, they will see a screen similar to this one:

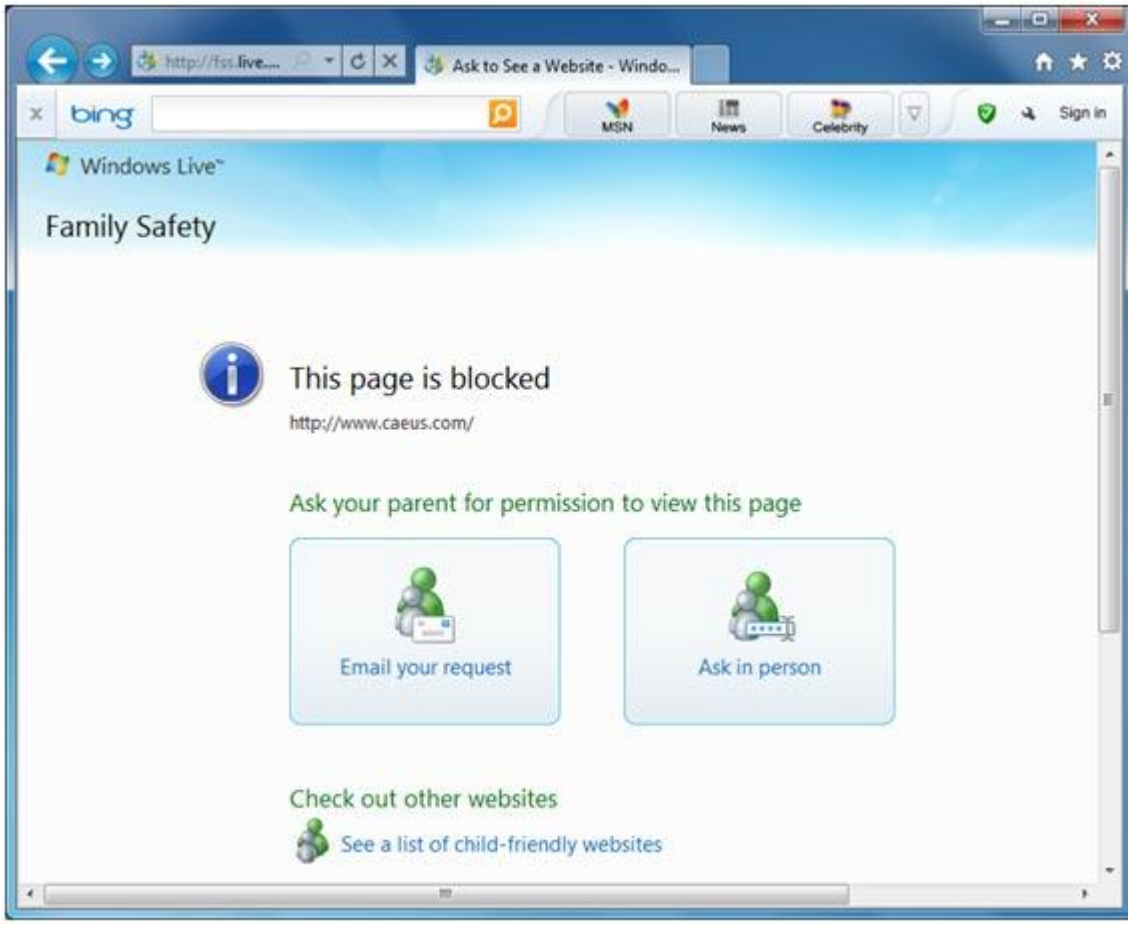

Figure 13 Page Blocked Message

If you are in the room, you may choose to allow access to the web site by pressing the **Ask in person** button. This then allows you to enter your Windows Live ID password (which may be different from the password you use to log on to your account on the computer) to permit access to the site.

Otherwise, if your child has reason to believe that the site is being blocked in error, they may send an email request which you may review and take appropriate action.

You may also view logs of each account's activity to see what your children have been up to, and restrict access to various contacts by using the appropriate screen as selected from the left-hand menu within the web-based settings interface.

4.0 Additional Rules to help protect your children's privacy and safety on the Internet

You can follow the following steps, in addition to parental controls, to protect your children's privacy and safety when they are online.

Step 1. Decide where your child can and can't go on the Internet

It is a good idea to visit some sites for kids. Pay particular attention when sites collect personal information.

Read the privacy statement and, if you don't agree with it, do some research, to find a similar site that doesn't request personal information.

- **Block inappropriate content**

  One of the best defenses against inappropriate content is to block it before you see it. With Microsoft software there are a few different ways you can do this.

- **Windows Live Family Safety.**

  This software helps you filter information based on each child's age. You can also limit searches, block or allow certain websites, and monitor what your kids do online. You also have access to guidelines on how to help a child use online communications safely or how to talk to children about inappropriate web browsing. For more information, see **Windows Live Family Safety**.

- **Xbox parental controls.**

  Xbox includes parental controls that help you restrict your child's ability to play inappropriate games and watch inappropriate DVD movies.

  For more information, read **Parental Controls: Software settings to help keep kids safe.**

Step 2: Increase your security and privacy

In addition to blocking inappropriate content, it's a good idea to block sites and downloads that might be a risk to your security and privacy.

- **Set limits on downloads.**

  Free games, free music, animated toolbars, and other downloads can expose your computer to **spyware** or other unwanted software. Depending on the ages of your children, you can teach them not to download software from unknown sources on the Internet or ask your permission before they download anything. This can help to keep unwanted software off of your computer.

  A child might accidentally infect your computer with spyware or other unwanted software. Some popular sites for kids might try to download programs without permission. To avoid this, monitor where your kids go online. For more information, see Step 3.

- **Use antivirus and antispyware software like Microsoft Security Essentials. Microsoft Security Essentials**

  These help you detect, disable, or remove viruses, spyware and other potentially unwanted software. You can download it for free for Windows 7, Windows Vista, and Windows XP.

- **Create different user accounts. Windows 7**, **Windows Vista**, and **Windows XP**

  These allow you to create multiple user accounts for your computer. Each user logs on with a unique profile and his or her own Desktop and My Documents folder. You can give yourself an Administrator account and give your children Limited User accounts. Administrator accounts have full control over the computer. Limited Users cannot change system settings or install new hardware or software, including most games, media players, and chat programs.

- **Adjust web browser security settings.**

  You can help protect your child through your web browser. Internet Explorer helps you control your security and privacy preferences by allowing you to assign security levels to websites.

Step 3: Monitor where your kids go online

It might not be possible to be present whenever your children are online. But it is possible to check later to see where your children have spent their time online.

By reviewing the History list in Internet Explorer, you can see all the places your children visited online. To view your Internet History, click the History button on the browser toolbar.

- **Windows Live Family Safety** and the parental controls in **Windows 7** and **Windows Vista** can also help you monitor where your kids go online.

Step 4: Remind kids not to talk to strangers online

Real-time chats, social networking, and instant messaging can be a great way for children to discuss their interests and build friendships. But the anonymity of the Internet can also put children at risk of falling victim to imposters and **predators**. To help minimise your children's vulnerability, teach them to take precautions such as:

- Use only a first name or nickname to identify themselves.
- Never disclose a phone number or address.
- Never send photographs of themselves.
- Never agree to meet someone they met online without supervision.

To help protect your children from being contacted by strangers while instant messaging, configure your software to allow only approved contacts.

4.0 Conclusion

Parental controls can be marvellous tools in helping to protect children, but they are not an alternative for parental involvement in online security awareness and education. Online safety issues such as sexting and cyberbullying may involve technology, but are in fact behavioural issues. There is no such tool that parents can download to fix behavioural problems. However, parental controls can be an important part of addressing online behaviour problems by alerting parents about these and blocking access to Internet resources that are potentially harmful.

5.0 References

- Caeus.com Ltd.
- Microsoft Website
- Parental Controls Product Guide 2010