CYBERSAFETY POLICY

Rationale

St Mark's Lutheran School has a duty of care to ensure the safety of all students and staff. This involves the provision of a safe physical and emotional environment for students and staff.

The internet is a world wide phenomenon that provides access to a continuously growing wealth of knowledge and information. This information comes from a vast range of sources including private and public institutions as well as individuals. The educational value of the information available on the Internet is significant; however, this also includes information of questionable educational value, not to mention information that is inaccurate, abusive, offensive or illegal.

It is the desire of St. Mark's to support students in becoming responsible and discerning users of the Internet. It is the joint responsibility of the school and the parents of each student to educate the student about his or her responsibilities when using the various forms of Information Communication Technology now available at our fingertips. Use of ICT resources by students outside of school hours remains the responsibility of the parents.

The students of St Mark's are expected to use the school's ICT resources in a manner consistent with this policy and they will be held accountable and responsible for their use. St Mark's has an '*Acceptable Use Policy*' and procedural guidelines for accessing and using the Internet at school for all students from Reception to Year 7. We urge all parents to discuss the contents of the policy with their children prior to signing the agreement to ensure that they and their child are aware of the legal and School implications of any breaches to the policy.

Further information, including tips and guidelines for safe Internet use in the home environment can be found at the Australian Government website (www.cybersmart.gov.au). Free home filtering software is also available from this site.

Aim

St Mark's will develop and maintain rigorous and effective cybersafety practices which aim to maximise the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimising and managing any risks.
These cybersafety practices will aim to not only maintain a cybersafe school environment, but also aim to address the need of students and other

members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.

Implementation

No individual may use the school Internet facilities and school-owned devices/equipment in any circumstances unless the appropriate use agreement has been signed and returned to the school. Use agreements also apply to the use of privately-owned ICT equipment on the school site, or at/for any school-related activity, regardless of its location. This includes off-site access to the school network from school or privately-owned equipment.

St Mark's use agreements will cover all employees and all students, and any other individuals authorised to make use of the school Internet facilities and ICT devices/equipment.

The use agreements are also an educative tool and should be used as a resource for the professional development of staff and the education of students in safe and responsible use of ICT equipment.

Use of the Internet and the ICT equipment by staff, students and other approved users at St Mark's is to be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements.

Signed use agreements will be filed in a secure place, and an appropriate system devised which facilitates confirmation that particular individuals are authorised to make use of the Internet and ICT equipment.

The school has the right to monitor, access and review all use. This includes personal emails sent and received on the schools computer/s and/or network facilities at all times.

The school has the right to audit at anytime any material on equipment that is owned by the school. The school may also request permission to audit privately owned ICT equipment used on the school site or at any school related activity.

The safety of children is of paramount concern. Any apparent breach of cybersafety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the school's cybersafety practices. In serious incidents, advice will be sought from an appropriate source, such as someone with specialist knowledge in this area. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If illegal material or activities are suspected, the matter will need to be reported to relevant law enforcement.

Date policy adopted by St Mark's Lutheran School Council: …….

Chairperson: ……

Principal: ……

Review This policy will be reviewed at least every 3 years.

St Mark's
LUTHERAN SCHOOL
MOUNT BARKER

STAFF CYBERSAFETY USE AGREEMENT

INTRODUCTION
This document consists of this cover page and two sections.

SECTION A – Important Cybersafety Initiatives and Rules

SECTION B – Some Important Staff Obligations Regarding Student Cybersafety

SECTION C – Staff Cybersafety Use Agreement Form.

INSTRUCTIONS FOR STAFF

1. Please read all documentation carefully. If help is needed to understand the language, or clarification on any items, please speak to a member of the ICT Committee.
2. Detach Section C, sign and return it to the school office.
3. Please keep this policy for future reference.

Important terms used in this document:

- The abbreviation '**ICT**' in this document refers to the term 'Information and Communication Technologies'.
- '**Cybersafety**' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.
- '**School ICT**' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below.
- The term '**ICT equipment/devices**' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other technologies as they come into use.

SECTION A

THE ROLE OF USE AGREEMENTS IN ST MARK'S LUTHERAN SCHOOL CYBER SAFTEY PROGRAM

The values promoted by St Mark's Lutheran School include **respect** (we are considerate of others, honour their role and recognise their worth as individuals) in an environment which is physically and emotionally safe. The measures to ensure the cybersafety of the school environment which are outlined in this document are based on these core values.

The school's computer network, Internet access facilities, computers and other school ICT equipment/devices provide exciting opportunities to expand the teaching and learning programs at St Mark's Lutheran School, and are imperative to the effective operation of the school. However, it is essential that the school support the safe and responsible use of ICT equipment through the education of students and preventative measures.

Therefore St Mark's Lutheran School has cybersafety practices in place, which include cybersafety use agreements for all school staff and students.

Cybersafety use agreement documents include information about obligations and responsibilities, and the nature of possible consequences associated with breaches of the use agreement which undermine the safety of the school environment. The cybersafety education of students is designed to complement and support the use agreements. The overall goal of the school in this matter is to help keep the students cyber safe by creating and maintaining a cybersafety culture which is in keeping with the values of the school, as well as legislative, and professional, obligations. All members of the school community benefit from being party to the use agreements and other aspects of the school cybersafety program.

1. CYBERSAFETY USE AGREEMENTS

1.1. All staff and students, whether or not they presently make use of school ICT, will be issued with a use agreement. Staff are required to read these pages carefully, and return the signed agreement form **Section C** to the school office for filing.

2. REQUIREMENTS REGARDING APPROPRIATE USE OF ICT IN THE SCHOOL

2.1. The use of St Mark's computer network, Internet access facilities, computers and other ICT equipment/devices is limited to educational and creative purposes which is both reasonable and appropriate to the school environment.

2.2. Any staff member who has a signed use agreement with the school and allows another person who does not have a signed use agreement to use the school ICT, is responsible for that use.

2.3. The use of privately owned ICT equipment / devices on the school site, or at any school related activity must be appropriate to the school environment. This includes any images

or material present/stored on privately owned ICT equipment / devices brought onto the school site, or to any school-related activity. This also includes the use of mobile phones.
*Note that examples of a **'school-related activity'** include, but are not limited to, an excursion, camp, sporting or school community event, wherever its location.*

2.4. The school takes all reasonable precautions to screen material being accessed through information systems such as the Internet. However, it may not always be possible for the school to filter or screen all material. This may include material which is **inappropriate** in the school environment.
It is the expectation that each individual will make responsible use of such systems.

3. MONITORING BY THE SCHOOL

3.1. The school monitors traffic and material sent and received using the school's ICT infrastructures. This may be examined and analysed to help maintain a cyber safe school environment when the need arises.

3.2. St Mark's has the right to monitor, access, and review all the use detailed in 2.1, 2.2 & 2.3. This includes personal emails sent and received on the school's computers and/or network facilities, either during or outside school hours if a need arises.

3.3. The school will deploy filtering and/or monitoring software where appropriate to restrict access to certain sites such as social networking and web based email.
However, where there is educational value in accessing such sites, arrangements can be made by contacting the ICT Coordinator or Business Manager to enable you to do so.

4. AUDITS

4.1. The school will occasionally conduct an internal audit of its computer network, Internet access facilities, computers and other school ICT equipment/devices, or may commission an independent audit.

4.2. Where deemed necessary stored content will be deleted. Staff and students will be notified prior to this taking place.

5. All material submitted for publication on the school website/intranet should be appropriate to the school environment. Such material can be posted only by those given the authority to do.

6. All ICT equipment/devices should be cared for in a responsible manner. Any damage, loss or theft must be reported immediately to the ICT Coordinator or Business Manager.

7. All users are expected to practice sensible use to limit wastage of computer resources or bandwidth. This includes unnecessary printing, unnecessary Internet access and unnecessary storing of data (i.e. photos).

8. The users of school ICT equipment & devices must comply with copyright and licensing agreements relating to original work. Users who infringe copyright may be personally liable.

9. Staff network passwords must be strong (i.e. A strong password is between 6-8 characters and includes letters & numerals), kept confidential and not shared with anyone else.

10. Any electronic data or files such as units of work, reports, policies; created or modified on behalf of St Mark's Lutheran School on any ICT, regardless of who owns the ICT, are the property of St Mark's Lutheran School.

11. DEALING WITH INCIDENTS

11.1. Staff must inform the ICT Coordinator or Business Manager should an incident occur.

11.2. Any incident involving the unintentional or deliberate accessing of inappropriate material by staff or students, will be recorded and filed in a central location by the Business Manager.

11.3. In the event of access to such material, users should:
1. Not show others
2. Close or minimize the window, and
3. Report the incident as soon as practical to the ICT Coordinator or Business Manager.

11.4. If an incident involves inappropriate material or activities of a serious nature, or is suspected of being illegal, it is necessary for the incident to be reported to the ICT Coordinator and Business Manager immediately.

12. BREACHES OF THIS AGREEMENT

12.1. Breaches of the use agreement can undermine the values of the school and the safety of the learning environment, especially when ICT is used to facilitate misconduct. Such a breach which is deemed harmful to the safety of the school (for example, involvement with inappropriate material, or anti-social activities like harassment), may constitute a significant breach of discipline and possibly result in serious consequences. The school will respond to any breach of the use agreement in an appropriate manner taking into account all relevant factors on a case by case situation.

12.2. If there is a suspected breach of use agreement involving privately-owned ICT e.g. (USB flash drive) on the school site or at a school related activity, the matter may be investigated by the school. The school may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.

12.3. Involvement with material which is deemed inappropriate in a school setting, is a very serious matter, as is involvement in an activity which might constitute criminal misconduct, such as cyber bullying. In such situations it may be necessary to involve law enforcement in addition to any disciplinary response made by the school.

13. QUERIES OR CONCERNS

13.1. Staff should take any queries or concerns regarding technical matters to the ICT Coordinator or Business Manager.

13.2. Queries or concerns regarding other cybersafety issues, should be taken to the ICT Coordinator or Business Manager.

13.3. In the event of a serious incident which occurs when the ICT Coordinator or Business Manager are not available, another member of the leadership team should be informed immediately.

SECTION B

IMPORTANT STAFF REQUIREMENTS REGARDING STUDENT CYBERSAFTEY

1. Staff have the professional responsibility to ensure the safety and wellbeing of children using the school's computer network, Internet access facilities, computers and other school ICT equipment/devices on the school site or at any school-related activity.

2. If staff are aware that a student has not signed a use agreement, the student will not be permitted to use school ICT equipment /devices unless there are special circumstances approved by the principal.

3. If staff are aware of any students who have not signed a use agreement their names should be reported to the ICT Coordinator or Business Manager.

4. Staff should guide students in effective strategies for searching and using the Internet.

5. While students are accessing the Internet in a classroom situation, the supervising staff member should be an active presence.

6. Staff should support students in following the student use agreement. This includes:

    a. Endeavouring to check that all students in their care understand the requirements of the student agreement.

    b. Regularly reminding students of the contents of the use agreement they have signed, and encouraging them to make positive use of ICT equipment/devices.

SECTION C

ST MARK'S LUTHERAN SCHOOL STAFF CYBERSAFETY USE AGREEMENT FORM

Please complete, sign, and date this Staff Use Agreement Form which confirms your agreement to follow the obligations and responsibilities outlined in this document. If you have any queries about the agreement, you are encouraged to discuss them with the ICT Coordinator or the Business Manager before you sign. Once signed, this form should be returned to the school office for filing with staff records.

A copy of the signed form will be supplied to you.
This year the ICT Coordinator at St Mark's Lutheran School is……

USE AGREEMENT

I have read and am aware of the obligations and responsibilities outlined in this Staff Cybersafety Use Agreement document, a copy of which I have been advised to retain for future reference. These obligations and responsibilities relate to the cybersafety of students in the school community.

I also understand that breaches of this Staff Cybersafety Use Agreement will be investigated and could result in disciplinary action, and where required, referral to law enforcement

.

Name: ……

Role in the school:……..

Signature:……Date:.....

STUDENT CYBERSAFETY POLICY

INTRODUCTION
This document consists of this cover page and two sections.

SECTION A – The role of Use Agreements in St Mark's Lutheran School Cybersafety Program; and Cybersafety Rules for students, including explanatory notes for parents*/legal guardians/caregivers.

SECTION B – Cybersafety Use Agreement Form

INSTRUCTIONS FOR PARENTS*/LEGAL GUARDIANS/CAREGIVERS

1. Please read all documentation carefully. If help is needed to understand the language, or clarification on any items, please contact the school.
2. Discuss the Cybersafety Rules with your child.
3. Both you and your child should sign the Use Agreement and return to the school office.
4. Please keep this policy for future reference.

* The term 'Parent' used throughout this document also refers to legal guardians and caregivers.

Important terms used in this document:

- The abbreviation '**ICT**' in this document refers to the term 'Information and Communication Technologies'.
- '**Cybersafety**' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.
- '**School ICT**' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below.
- The term '**ICT equipment/devices**' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other technologies as they come into use.

SECTION A

THE ROLE OF USE AGREEMENTS IN ST MARK'S LUTHERAN SCHOOL CYBERSAFTEY PROGRAM

The values promoted by St Mark's Lutheran School include **respect** (we are considerate of others, honour their role and recognise their worth as individuals) in an environment which is physically and emotionally safe. The measures to ensure the cybersafety of the school environment which are outlined in this document are based on this core value.
The school's computer network, internet access facilities, computers and other school ICT equipment/devices provide exciting opportunities to expand the teaching and learning programs at St Mark's Lutheran School, and are imperative to the effective operation of the school. However, it is essential that the school support the safe and responsible use of ICT equipment through the education of students and preventative measures.
Therefore St Mark's Lutheran School has cybersafety practices in place, which include cybersafety use agreements for all school staff and students.
Cybersafety use agreement documents include information about obligations and responsibilities, and the nature of possible consequences associated with breaches of the use agreement which undermine the safety of the school environment. The cybersafety education of students is designed to complement and support the use agreements. The overall goal of the school in this matter is to help keep the students cyber safe by creating and maintaining a cybersafety culture which is in keeping with the values of the school, as well as legislative, and professional, obligations. All members of the school community benefit from being party to the use agreements and other aspects of the school cybersafety program.

POLICY STATEMENTS
Some of the information in this section is less likely to apply to junior primary students while at school, however, it is helpful for parents to be aware of the scope of this important, school-wide, cybersafety initiative. It also provides parents with valuable material to assist them in their efforts to keep their children cybersafe in the home.

1. CYBERSAFETY USE AGREEMENTS

1.1 All staff and students, whether or not they presently make use of school ICT, will be issued with a use agreement. Parents are required to read these pages carefully, and return the signed agreement to the school office for filing.

2. REQUIREMENTS REGARDING APPROPRIATE USE OF ICT IN THE SCHOOL LEARNING ENVIRONMENT

In order to meet the school's legislative obligation to maintain a safe physical and emotional learning environment, and be consistent with the values of the school:

2.1 The use of St Mark's computer network, Internet access facilities, computers and other ICT equipment/devices is limited to educational and creative purposes appropriate to the school environment.

2.2 St Mark's has the right to monitor, access, and review all the use detailed in 2.1. This includes personal emails sent and received on the school's computers and/or network facilities, either during or outside school hours if a need arises.

2.3 The use of privately-owned ICT equipment/devices on the school site, or at any school-related activity must be appropriate to the school environment. Equipment/devices could include a mobile phone, camera, recording device, or portable storage (like a USB or flash memory device). Anyone unsure about whether or not it is appropriate to have a particular device at school or at a school-related activity, or unsure about whether the planned use of a particular device is appropriate, should check with the teacher and/or ICT Coordinator.

*Note that examples of a **'school-related activity'** include, but are not limited to, an excursion, camp, sporting or school community event, wherever its location.*

2.4 The school takes all reasonable precautions to screen material being accessed through information systems such as the Internet. However, it may not always be possible for the school to filter or screen all material. This may include material which is **inappropriate** in the school environment.

It is the expectation that each individual will make responsible use of such systems.

3. MONITORING BY THE SCHOOL

3.1 The school monitors traffic and material sent and received using the school's ICT infrastructures. This may be examined and analysed to help maintain a cybersafe school environment when the need arises.

3.2 The school will deploy filtering and/or monitoring software where appropriate to restrict access to certain sites such as social networking and web based email.(MySpace, Hotmail, Facebook etc.)

However, as in 2.4, the expectation is that each individual will be responsible in their use of ICT equipment.

3.3 Users must not attempt to circumvent monitoring or filtering.

4. AUDITS

4.1 The school will occasionally conduct an internal audit of its computer network, Internet access facilities, computers and other school ICT equipment/devices, or may commission an independent audit.

4.2 Where deemed necessary stored content will be deleted. Staff and students will be notified prior to this taking place.

5. BREACHES OF THIS AGREEMENT

5.1 Breaches of the use agreement can undermine the values of the school and the safety of the learning environment, especially when ICT is used to facilitate misconduct.

Such a breach which is deemed harmful to the safety of the school (for example, involvement with inappropriate material, or anti-social activities like harassment), may constitute a significant breach of discipline and possibly result in serious consequences. The school will respond to any breach of the use agreement in an appropriate manner, taking into account all relevant factors on a case by case situation.

Depending on the seriousness of a particular breach, possible school responses could include one or more of the following: a discussion with the student, informing parents, loss of ICT privileges, the family possibly having responsibility for the cost of ICT repairs or replacement, the school taking disciplinary action which are outlined within the school's behaviour management policy.

5.2 If there is a suspected breach of use agreement involving privately-owned ICT e.g. (USB flash drive) on the school site or at a school related activity, the matter may be investigated by the school. The school may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.

5.3 Involvement with material which is deemed inappropriate in a school setting, is a very serious matter, as is involvement in an activity which might constitute criminal misconduct, such as cyber bullying. In such situations parents will be contacted and it may be necessary to involve law enforcement in addition to any disciplinary response made by the school.

6. OTHER ASPECTS OF THE SCHOOL'S CYBERSAFETY PROGRAMME

6.1 The use agreements operate in conjunction with other cybersafety initiatives, such as cybersafety education supplied to the school community. This education plays a significant role in the school's overall cybersafety program, helping students to be cybersafe in all areas of their lives.

7. CYBERSAFETY RULES FOR YEAR R-7 STUDENTS

Note for Parents/Legal Guardians/Caregivers:
The sections 7.1-7.25 are designed to provide a guide to the rules covered by this use agreement, and to help you discuss the rules with your child. Teachers will also outline to students their responsibilities when using the schools ICT equipment and network.

The meaning of 'ICT' or 'ICT equipment/devices' can be found on page one.

7.1 I must have a use agreement signed by me and by my parent or caregiver before I am allowed to use the school ICT equipment.

- *All students, regardless of age or ability, must have a use agreement signed by their parent. All students sign their use agreements along with their parents. Use agreements are becoming accepted as an essential part of cybersafety policy and programmes for schools and other organisations, including businesses.*

7.2 I can use the school computers and other school ICT for uses the school deems appropriate.

- *This helps to ensure the equipment is available when students need to use it for their learning. It will also help to reduce the likelihood of any inappropriate activities taking place which put at risk the safety of the learning environment.*

7.3 If I am unsure whether I am allowed to do something involving ICT, I will ask the teacher first.

- *This helps the students of St Mark's to take responsibility for their own actions, and seek advice when they are unsure of what to do. It provides an opportunity for the teacher and student to work through an issue and so avoid the student making an unwise decision which could possibly lead to serious consequences. Young children need ongoing advice and guidance to help them become safe and responsible users of ICT.*

7.4 I will follow the cybersafety rules, and will not join in if others are being irresponsible. I will tell the teacher of such behaviours straight away.

- *Unfortunately, along with many benefits, technology has also provided new ways to carry out anti-social activities. Bullying and harassment by text message, for example, is becoming a major problem in Australia and in many other countries. Often children become involved in these acts through peer pressure, without thinking of the consequences.*

7.5 If I accidentally come across mean, rude, or dangerous material I will tell the teacher straight away, without showing any other students. The teacher will then notify the network administrator to block this material.

- *Because anyone at all can publish material on the Internet, it does contain material which is inappropriate, and in some cases illegal. The school takes a number of steps to prevent this material from being accessed. However, there always remains the possibility that a student may inadvertently stumble across something inappropriate. Encouraging students to tell a teacher immediately if they find something which they suspect may be inappropriate, encourages critical thinking and helps students to take responsibility for their actions and keep themselves, and others, safe. This way, they contribute to the cybersafety of the school community.*

7.6 If I am not feeling safe at any time while using the ICT equipment, I will tell the teacher straight away.

- *St Mark's strives to create a safe and secure learning environment for all members of the school community. Examples of situations involving the use of ICT which might cause a student to feel unsafe could include: contact being made by a stranger through email or text message, the presence of 'scary' images on a computer screen, and/or misconduct by other students. Staff need to be made aware of such situations as soon as they occur to ensure the school can respond immediately.*

7.7 I will only log onto the school network using my user account.

7.8 I will not share my password with any other person.

- *Passwords perform two main functions. Firstly, they help to ensure only approved persons can access the school ICT facilities. Secondly, they are used to track how those facilities are used. Knowing how the equipment is being used and by whom, helps the school to maintain a cybersafe environment for all users, and teaches the student the importance of personal security.*

7.9 I will log off or shut down the computer when I have finished using it.

7.10 I will log off before letting someone else use the computer.

- *Logging off or shutting down, stops others from using a computer under your child's username. When the computer is started up again, the next user has to enter their own details to log on.*

7.11 If I am sharing a computer which is logged on under my name/by me, I am responsible for how it is used. If there is a problem, I will tell the teacher immediately.

- *Students often work together at a single computer. It is important that your child takes responsibility for sensible use of the computer at all times, and tells the teacher if there is any concern.*

7.12 I will check with the teacher before giving anyone information about myself or others when using the Internet – this includes name, home and email addresses, and phone numbers.

- *This reduces the risk of students being contacted by someone who wishes to upset or harm them, or use their identity for purposes which might compromise the student's privacy or security online.*

7.13 I will not be careless, try to damage, or steal any school ICT equipment. (If this happens, the school will need to inform my parents about what has happened. My parents may have responsibility for the cost of repairs or replacement.)

7.14 I will not try to stop the network or any other equipment from working properly.

7.15 If I accidentally break school ICT equipment, damage it through mishandling, or I find it broken when I start to use it, I will tell a teacher straight away.

7.16 I will not change any screensavers, desktop backgrounds, themes or hardware settings.

7.17 I will have no involvement with making or sending malware (such as viruses, worms & trojans) on purpose.

7.18 I will use good judgement to decide whether printing is necessary. If I am unsure I will seek advice from a teacher.

- *Rules 12-18 are designed to help protect the investment the school has made in expensive ICT technologies. Also, certain settings may have been applied to maximise the safety of the students and the equipment (such as antivirus settings or restrictions on Internet access).*

7.19 I will not download any files such as music, videos, or programs.

- *Many files available on the Internet are covered by copyright, and although they can be easily downloaded, it may be illegal to do so. Sometimes even innocent-looking files may contain malicious content such as viruses, or spyware (software that searches for personal information from your computer and transmits it to others over the Internet). As well, some files may contain inappropriate or illegal material.*

7.20 I must have permission from school, before bringing any disk or other ICT equipment / device from home. If I am given permission, then I must use that ICT sensibly.

- *The devices referred to in this rule include those specified on page one of this document; for example flash memory devices, iPods, MP3 players or mobile phones. Any students bringing such devices from home are asked to use them sensibly. This applies to the school site, and any school-related activity.*

  This rule is designed to protect the school's online security and equipment from viruses which can easily be transferred using disks or other storage devices such as memory cards.

  NB Parents should be mindful of the school's specific policy regarding students and mobile phones.

  You might like to take this opportunity to have a discussion with your child about their general use of ICT whether in or out of school. It helps keep children cybersafe if they understand that many of these rules should be followed regardless of whose ICT equipment they are using, where they are (for example at home, at school, or at a friend's house), or who they are with.

7.21 I will not bring software or games from outside school to use on school equipment.

- *Installing software from home may cause conflicts with the software installed by the school. St Mark's Lutheran School must also abide by any licensing requirements included within the software. This means that unless the school has purchased a copy, it will not usually be legally entitled to install the software. And as mentioned in point 19, inappropriate or illegal content may be involved.*

7.22 I will acknowledge where work has come from if I have copied it from somewhere. This includes graphics and sounds files I use in my own schoolwork.

- *The Internet has allowed easy access to a huge range of information which can be incorporated into students' work by simply cutting and pasting. Most of this material is copyrighted, and thus involves intellectual property issues. Also, the value to students' learning is questionable if they have not thought through this information themselves.*

7.23 I will check with the teacher before using school equipment to copy software, music, videos or other files, in case they are copyrighted.

- *Any such copying is likely to be restricted by copyright laws. St Mark's Lutheran School cannot condone the use of its equipment for these activities.*

7.24 I will not use the internet, mobile phones or any other ICT equipment to be mean, rude, offensive, or to harass any members of the school community like students and staff, while at school or when involved in any school-related activity. The same rule applies when using school ICT at any time, whether at school or not.

- *The basic principles of respect extend to the use of information and communication technologies.The capacity of ICT to increase the scale and scope of misconduct can make an otherwise minor rule infringement into a much more serious matter. For example, name calling often becomes a more serious issue where texting or emailing has been used to facilitate harassment. Cyberbullying can involve a range of misconduct including the creation of abusive websites.*

7.25 If I break these rules, the school may need to talk to my parents about what has happened. Disciplinary action should be expected.

- *Depending on the seriousness of a particular breach, possible school responses could include one or more of the following: a discussion with the student, informing parents, loss of ICT privileges, the parents possibly having responsibility for the cost of ICT repairs or replacement, the school taking disciplinary action.*

SECTION B

CYBERSAFETY USE AGREEMENT FORM

TO THE STUDENT AND PARENT/LEGAL GUARDIAN/CAREGIVER:

- Please read this page carefully as it includes information about your responsibilities under this agreement.
- Complete and sign the appropriate section.
- Detach and return **Section B** to the school office.
- Keep **Section A** for your future reference.

ST MARK'S LUTHERAN SCHOOL WILL:

- do its best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or school ICT equipment/devices at school or at school-related activities
- work with children and their families to encourage and develop an understanding of the importance of cybersafety through education designed to complement and support the use agreement initiative. This includes providing children with strategies to help keep themselves safe in cyberspace
- keep a copy of this signed use agreement form on file
- respond to any breaches in an appropriate manner
- welcome enquiries from parents or students about cybersafety issues.

Student's section

MY RESPONSIBLITIES INCLUDE:

- I will read this Cybersafety Use Agreement document carefully with my parent or caregiver
- I will follow the cybersafety rules and instructions whenever I use school ICT
- I will also follow the cybersafety rules and instructions whenever I am involved with privately-owned ICT on the school site or at any school-related activity
- I will have no involvement in use of ICT which could put me at risk, or other members of the school community
- I will take proper care when using computers and other school ICT equipment/devices. If I have been involved in the damage, loss or theft of ICT equipment/devices, my parents may have responsibility for the cost of repairs or replacement
- I will ask my teacher or my parents if I am not sure about something to do with this agreement.

I have read and understand my responsibilities, and agree to follow the Cybersafety Use Agreement. I know that if I breach this use agreement, there may be serious consequences.

Name of student: _____ Class: _____

Signature: _____ Date: _____

Section for parent/legal guardian/caregiver

MY RESPONSIBLITIES INCLUDE:

- I will read this School Cybersafety Use Agreement document and discuss the rules with my child
- I will ensure this use agreement is signed by my child and by me, and returned to the school.
- I will support the school's cybersafety program by encouraging my child to follow the cybersafety rules, and to always ask the teacher if they are unsure about any use of ICT
- I will contact the School to discuss any aspect of this use agreement which I might want to learn more about.
- I will take every precaution to ensure that any file transferred to the school is virus free.

I have read this Cybersafety Use Agreement and am aware of the school's initiatives to maintain a cybersafe learning environment, including the responsibilities involved.

Name: _____

Parent/Legal Guardian/Caregiver (please circle which term is applicable)

Signature: _____ Date: _____