CYBER-SAFETY POLICY - McLAREN FLAT PRIMARY SCHOOL

Policy Purpose: To maximise learning opportunities and outcomes, while minimising the risk to students' safety and wellbeing

Dear Parent/Caregiver,

South Australian schools are exciting places in which to teach and learn: our children naturally take advantage of developments in technologies to personalise and expand their learning opportunities, and our educators provide rich learning environments for children as they engage with people and resources, locally and globally. In this dynamic, connected world of communication and learning, we need to ensure such opportunities do not place the young people in our schools and preschools at risk. Many of these risks are not new and educators are familiar with strategies and processes that maximise learning opportunities and outcomes, while minimising risk to children's safety and wellbeing.

The measures to ensure the cyber-safety of McLaren Flat Primary School are based on our core values of resilience, responsibility, pride, respect and honesty. To assist us to enhance learning through the safe use of information and communication technologies (ICTs), we are now asking you to read this policy document and sign the attached User Agreement Form.

Rigorous cyber-safety practices are in place, which include the responsibilities listed in this policy and cyber-safety User Agreements for staff and students. Child protection education, such as the Keeping Safe child protection curriculum, includes information about remaining safe when using new technologies and is provided to all students.

The computer network, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs at McLaren Flat Primary School, and to the effective operation of the school. The ICT equipment is for educational purposes appropriate to this environment, whether it is owned or leased either partially or wholly by the school, and used on or off the site.

The overall goal of this policy is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The policy includes information about your obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment. It is an expectation that all members of our school community will follow this policy.

Parents/caregivers should not post any photos, of other students, online in any form. This refers to photos/film taken during any school activity. Please remember that some students may have a court order prohibiting publication of their name or image.

All students will be issued with a copy of this policy and a User Agreement and once signed consent has been returned to school, students will be able to use the school ICT equipment. Conditions of this policy will be revisited with students at the beginning of each school year.

Material sent and received using the network may be monitored and filtering and/or monitoring software may be used to restrict access to certain sites and data, including e-mail. Where a student is suspected of an electronic crime, this will be reported to the South Australia Police. Where a personal electronic device such as a mobile phone, iPad, gaming console is used to capture images of a crime, such as an assault, the device will be confiscated and handed to the police.

While every reasonable effort is made by schools and DECD administrators to prevent children's exposure to inappropriate content when using the department's online services, it is not possible to completely eliminate the risk of such exposure. In particular, DECD cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. DECD recommends the use of appropriate Internet filtering software on home or personal devices.

More information about Internet filtering and cyber safety can be found on the websites of the Australian Communications and Media Authority at http://www.acma.gov.au , https://esafety.gov.au (formerly cybersmart), the Kids Helpline at http://www.kidshelpline.com.au and Bullying No Way at http://www.bullyingnoway.gov.au .

Please contact the Principal, if you have any concerns about your child's safety in using the Internet and ICT equipment/devices.

Important terms:
'Cyber-safety' refers to the safe use of the Internet and ICT equipment/devices, including mobile phones.

'Cyber bullying' is bullying which uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as e-mail, chat room discussion groups, instant messaging, webpages or SMS (text messaging) - with the intention of harming another person.

'School and preschool ICT' refers to the school's or preschool's computer network, Internet access facilities, computers, and other ICT equipment/devices as outlined below.

'ICT equipment/devices' includes 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 and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies.

'Inappropriate material' means material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school or preschool environment.

'E-crime' occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

Strategies to help keep McLaren Flat Primary Students Cyber-safe

Student responsibilities -
Students agree to the following policy conditions :

1. I will not use school ICT equipment until my parents/caregivers and I have signed my User Agreement Form and the completed form has been returned to school.

2. I will use the computers and other ICT equipment only for my learning.

3. I will go online or use the Internet at school only when a teacher gives permission and an adult is present.

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

5. If I have my own user name, I will log on only with that user name. I will not allow anyone else to use my name.

6. I will keep my password private.

7. I will use the Internet, e-mail, mobile phones or any ICT equipment only for positive purposes, not to be mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the school itself, even if it is meant as a joke.

8. While at school, I will:
   - attempt to search for things online that I know are acceptable at our school. This would exclude anything that is rude or violent or uses unacceptable language such as swearing
   - report any attempt to get around, or bypass, security, monitoring and filtering that is in place at our school.

9. If I find anything that upsets me, is mean or rude, or that I know is not acceptable at our school, I will:
   - not show others
   - turn off the screen
   - get a teacher straight away.

10. Only with written permission from home and approved by the school will I bring any ICT equipment/devices to school. This includes things like mobile phones, iPods, games, cameras, and USB/portable drives, iPads, tablets.

11. Only with permission from the teacher will I connect any ICT device to school ICT, or run any software (eg a USB/portable drive, camera or phone). This includes all wireless/Bluetooth technologies.

12. The school cyber-safety strategies apply to any ICTs brought to school.

13. To ensure my compliance with copyright laws, I will download or copy any files such as music, videos, games or programs only with the permission of a teacher or the owner of the original material.

14. I will ask my teacher's permission before I put any personal information online. Personal identifying information includes any of the following:
    - my full name
    - my address
    - my e-mail address
    - my phone numbers
    - photos of me and/or people close to me.

15. I will respect all school ICTs and will treat all ICT equipment/devices with care. This includes:
    - not intentionally disrupting the smooth running of any school ICT systems
    - not attempting to hack or gain unauthorised access to any system
    - following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with ICTs
    - reporting any breakages/damage to a staff member.
    - only use photographic equipment appropriately.

16. If I do not follow cyber-safety practices the school may inform my parents/caregivers. In serious cases, the school may take disciplinary action against me. My family may be charged for repair costs. If illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform the police and hold securely personal items for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.

✂ ....

CYBER-SAFETY USER AGREEMENT – Student acknowledgement

I have read this Cyber-safety User Agreement (or have had this read to me) and I am aware of my responsibilities:

Name of child...

Group/Class ....**Date**..

PLEASE TURN OVER TO COMPLETE PARENT ACKNOWLEDGEMENT

PLEASE RETURN THIS SECTION TO SCHOOL AND KEEP THE TOP SECTION FOR YOUR OWN REFERENCE.

Cyber-safety User Agreement Form

To the parent/caregiver/legal guardian:

> **Please read this page carefully to check that you understand your responsibilities under this agreement.**

> **Return the signed Use Agreement to the school.**

School responsibilities:
I understand that McLaren Flat Primary School will:

- do its best to enhance learning through the safe use of ICTs. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or on 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 cyber-safety through education designed to complement and support the policy initiative. This includes providing children with strategies to keep themselves safe in a connected online world
- respond to any breaches in an appropriate manner
- welcome enquiries at any time from parents/caregivers/legal guardians or children about cyber-safety issues
- comply with DECD policy – ICT Security.

Parent responsibilities include:

- discussing the information about cyber-safety with my child and explaining why it is important
- supporting the school's cyber-safety program by emphasising to my child the need to follow the cyber-safety strategies
- contacting the principal or nominee to discuss any questions I may have about cyber-safety and/or this policy.

✂ -

CYBER-SAFETY+
-USER AGREEMENT – Parent acknowledgement

I have read and understood this Cyber-safety User Agreement and I am aware of McLaren Flat Primary School's initiatives to maintain a cyber-safe learning environment.

Name of child...

Group/Class ....

Name of parent/caregiver/legal guardian..

Signature of parent/caregiver/legal guardian...Date...

> **Please note: This agreement will remain in force as long as your child is enrolled at this school.**
> **If it becomes necessary to add/amend any information or rule, you will be advised in writing.**

PLEASE TURN OVER TO COMPLETE STUDENT ACKNOWLEDGEMENT

PLEASE RETURN THIS SECTION TO SCHOOL AND KEEP THE TOP SECTION FOR YOUR OWN REFERENCE.