

### Email Address

At Kadina Memorial School we believe it is valuable for students in Years 3 – 12 to have their own email address. Students may use it to write to children in other classes, home, other schools (as penpals) and for small research projects. Older students will make far greater use of email within research that focuses around Information Literacy Skills. Staff monitor the appropriate use of email within the school. Students' email addresses are made of their first name (dot) surname and random numbers, eg tom.jones123.

**We encourage all parents to allow their child to have an email address.**

### DECD Guidelines for Media/Images

The Guidelines state that sites must ensure each child shown in the image has a signed consent form (attached to enrolment form). For instance, a photo of a group of students undertaking an activity cannot be used where six students have a consent form but one does not.

### Cyber Safety at Kadina Memorial School

The measures to ensure the cyber-safety of Kadina Memorial School are based on our core values. To assist us to enhance learning through the safe use of information and communication technologies (ICTs), we are now asking you to read this document and sign the attached Use Agreement Form.

Rigorous cyber-safety practices are in place, which include cyber-safety Use Agreements for staff and learners, who have been involved in the development of the agreement. 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 learners.

The computer network, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs at Kadina Memorial 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 Kadina Memorial School is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The Use Agreement 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.

All learners will be issued with a Use Agreement and once signed consent has been returned to school, learners will be able to use the school ICT equipment.

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.

While every reasonable effort is made by schools, preschools 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.

More information about Internet filtering can be found on the websites of the Australian Communications and Media Authority at <http://www.acma.gov.au>, NetAlert at <http://www.netalert.gov.au>, the Kids Helpline at <http://www.kidshelp.com.au> and Bullying No Way at <http://www.bullyingnoway.com.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.

## KMS Cyber-safety Use Agreement and Strategies for Middle and Secondary Students to help keep Kadina Memorial School Students Cyber-safe

Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices for themselves and the people around them regardless of the time of day. Being cyber-safe is no exception and we invite you to discuss with your child the following strategies to help us stay safe when using ICT at school and after formal school hours.

1. 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.
2. I will keep my password private.
3. While at school or working on a school related activity, I will inform my teacher of any involvement with any ICT material or activity that might put me or anyone else at risk (eg bullying or harassing).
4. 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.
5. I will use my mobile phone/s only at the times agreed to by the school during the school day.
6. While at school, I will:
  - access, attempt to access, download, save and distribute only age appropriate and relevant material
  - report any attempt to get around or bypass security, monitoring and filtering that is in place at school.
7. If I accidentally access inappropriate material, I will:
  - not show others
  - turn off the screen or minimise the window
  - report the incident to a teacher immediately.
8. To ensure my compliance with copyright laws, I will download or copy files such as music, videos, games or programs only with the permission of a teacher or the owner of the original material. If I infringe the Copyright Act 1968, I may be personally liable under this law. This includes downloading such files as music, videos, games and programs.
9. My privately owned ICT equipment/devices, such as a laptop, mobile phone, USB/portable drive *I bring to school or a school related activity*, also is covered by this User Agreement. Any images or material on such equipment/devices must be appropriate to the school environment.
10. 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.
11. 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.
12. The school may monitor traffic and material sent and received using the school's ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including e-mail.
13. The school may monitor and audit its computer network, Internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit. Auditing of the above items may include any stored content, and all aspects of their use, including e-mail.
14. If I do not follow cyber-safe 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.