Ph: (08)8853 2346 Fax: (08) 8853 2531 http://www.minlatonds.sa.edu.au/

We envision a learning environment where technology is a part of us, not apart from us.

Contents

1. Advice from DfE (Department for Education)

Opportunities for young people and adults to learn and engage with each other have exploded in recent times with the proliferation of computer networks, mobile devices, broadband connections to the Internet and virtual communities. With such exciting opportunities comes the need to ensure that leaders, educators, children and parents consider the implications for safe use of information and communication technologies (ICTs).

Learning is a social activity. It happens when people interact with other people and their ideas, knowledge and perspectives. ICTs provide children and students with new and engaging ways to learn. ICTs expand social and knowledge networks so that children and students access current information, interact with experts and participate in peer teaching and learning. Using ICTs they can publish their learning, as evidence of achievement or to invite feedback for improvement.

It is important to both protect children, students and adults, while they learn to use ICTs and teach them to become responsible digital citizens. This includes adults thinking ahead of new risks and children and students learning how to avoid exposure to inappropriate material or activities, and protecting themselves when they are online. They need to learn how to use ICTs, including mobile technologies and social networking sites, in responsible and ethical ways. In addition, they need to feel confident about alerting the adults in their lives when they are feeling unsafe, threatened, bullied or exposed to inappropriate events. In response, these adults need to take appropriate actions to protect the child or young person.

DfE and each of its schools and preschools make every reasonable effort to achieve this by:

- developing programs to educate and inform children, students and parents about the opportunities and challenges of ICTs in learning programs

- monitoring and logging e-mail traffic and Internet use, and providing filters to help guard against access to inappropriate materials
- providing direction and advice about ICTs (including the Internet and mobile phones) use and misuse, such as bullying and e-crime
- supporting police officers in undertaking an investigation and the collection of evidence following a principal or director reporting a suspected e-crime.

In matters relating to cyber-safety, DfE works with, and is advised by:

- the Keeping Safe: Child Protection Curriculum - a child protection teaching and learning program in South Australian government schools and preschools, developed by experienced South Australian educators and child protection experts.
- the Responding to Risks of Harm, Abuse and Neglect Training program (previously Mandatory Notification Training)
- the Australian Communications and Media Authority (ACMA), which manages a national cyber-safety education and awareness program and is also responsible for monitoring online content, including Internet and mobile phone content, and enforcing Australia's anti-spam law.
- South Australia Police (SAPOL)
- the Coalition to Decrease Bullying, Harassment and Violence in South Australian Schools, which has representatives from the three schooling sectors and eminent international researchers Professor Ken Rigby, Professor Phillip Slee and Drs Barbara Spears and Shoko Yoneyama.

2. Social Media

Social media are online services and tools used for publishing, sharing and discussing information. The list of social media types is extensive with new and innovative social media sites being developed almost every day. It is important to understand that social networking can occur in open and closed online communities. An open community on the web is visible to everyone worldwide. It is possible to have a closed community which restricts information and comments to a specific group of people.

Social Media platforms are dynamic and terms of use and licensing may change without notice. Online communication is critical to students learning of 21st Century skills, and tools such as blogging, podcasting, and chatting offer an authentic, real-world vehicle for student expression.

Student safety and care are the primary responsibility of teachers. Therefore, teachers need to ensure the use of Web interactive tools follows all established Internet safety guidelines.

The use of online document generators (*eg Google Docs*), blogs, podcasts or other web 2.0 and 3.0 tools is considered an extension of the classroom. Therefore, any speech that is considered inappropriate in the classroom is also inappropriate in all uses of blogs, podcasts, or other web 2.0 and 3.0 tools. This includes— but is not limited to—profanity, racist, sexist, or discriminatory remarks.

It is important that:

- Students using these tools are expected to act safely by keeping ALL personal information out of their posts.
- Students should NEVER post personal information on the web (including, but not limited to, last names, personal details such as address or phone numbers, or photographs).
- Students should NEVER, under any circumstances, agree to meet someone they have met over the Internet. Students should report such instances to their teacher or a responsible adult.
- Any personal blog a student creates must follow these blogging guidelines and the *DfE Social Media Guidelines.*
- Students should never link to web sites from their blog or blog comments without reading the entire article to make sure it is appropriate for a school setting.
- Students using such tools agree to not share their user name or password with anyone besides their teachers and parents and treat Web posting spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog.
- Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

3. Passwords

- Passwords are not for publication.
- Passwords should contain uppercase letters, lowercase letters and numbers.
- DO NOT use a common dictionary word or any aspect of your own name.
- Use substitute numbers for letters in words. For example, "DEVIL" could become "D3VIL"; "COFFEE" could become "COFF33".
- Try to think of a sentence or phrase and use the first letter of each word. For example, "my iPad 2 is the best" could become "mip2itb".
- From here, substitute some letters for capitals, numbers or symbols. For example, "mip2itb" could become "M!p2!tB".
- Add something on the end relating to the use for the password. For example, an iTunes account password could be "M!p2!tBTun".
- This gives a really strong password with a rating of 93% (checked using "The Password Meter" http://www.passwordmeter.com/).

4. Publishing

Technology provides an abundance of opportunities for users to utilise interactive tools and sites on public websites that benefit learning, communication, and social interaction. Users may be held accountable for the use of and information posted on these sites if it detrimentally affects the welfare of individual users or the governance, climate, or effectiveness of the school. From time to time, teachers may recommend and use public interactive sites that, to the best of their knowledge, are legitimate and safe. As the site is "public" and the teacher, school, and DfE are not in control of it, all Users must use their discretion when accessing information, storing, and displaying work on the site.

5. BYOD (Bring Your Own Device)

Minlaton District School believes that 21st Century instruction is necessary for 21st Century learning. Providing students with an environment that fosters and encourages this belief is part of our core values.

Our students are living in a world where they have immediate access to information anytime and anywhere. Many students have personally owned devices in their pockets that can be used to allow them to learn in their own style and at their own pace. With digital learning, every student can access high quality and rigorous instruction in every subject, thereby, maximizing their opportunity for success in school and beyond. A decade ago this was just a dream. Today, it can be a reality.

Minlaton District School recognises that when students feel connected to their device they are more likely to use it responsibility and holistically in the management and access of information to improve their overall learning.

With this in mind, the use of personal devices such as Laptops, iPods, iPads, tablets and other portable devices are encouraged when used in accordance with the policy outlined in this document. The maintenance and care of any device brought onto the school site remains *the sole responsibility of the student and their family.*

Any damage or loss remains the responsibility of the students, and the school accepts no liability in such cases.

Minlaton District School has a right to protect its network and technical resources. Any network user who brings his/her own personal device into the school is required to adhere to and sign a copy of the Minlaton District School BYOD Agreement.

Students and parents must complete a new form for each new device a student wishes to use at school.

6. Data Backup

It is the student's responsibility to ensure their data is regularly backed up. The method for backing up data is dependent on the device.

- Data created on a school-owned device should be saved to the student's Home Drive and backed up to a USB drive or portable Hard Disk.
- Data created on an iPad should be backed up by synchronising the iPad to iTunes on a computer at home OR by synchronising data to an iCloud space (available to students with an active Apple ID).
- Data created on a student-owned laptop should be backed up (by saving) to the student's Home Drive at school as well as backing it up to a portable device such as a USB or portable Hard Disk.

7. Appropriate Behaviour and Use POLICY

DfE ICT Security, Internet Access and Use, and Electronic Mail and Use policies contain the following main provisions. Children and students may use the Internet only for learning related activities that are approved by a teacher. They must ***not*** cause interference or disruption to other people or equipment, and children may ***not*** access or distribute inappropriate material. This includes:

- distributing spam messages or chain letters
- accessing or distributing malicious, offensive or harassing material, including jokes and images
- bullying, harassing, defaming or giving offence to other people
- spreading any form of malicious software (eg viruses, worms)
- accessing files, information systems, communications, devices or resources without permission
- using for personal financial gain
- using non-approved file sharing technologies (eg Torrent)
- using for non-educational related streaming audio or video
- using for religious or political lobbying
- downloading or sharing non-educational material.

Users must respect and protect the privacy of others by:

- Using only assigned accounts.
- Only viewing, using or copying passwords, data or networks to which they are authorised.
- Refraining from distributing private information about others or themselves.

Users must respect and protect the integrity, availability, and security of all electronic resources by:

- Observing all school internet filters and posted network security practices.
- Reporting security risks or violations to a teacher or network administrator.
- Not destroying or damaging data, networks, or other resources that do not belong to them.
- Conserving, protecting, and sharing these resources with other users.
- Notifying a staff member or administrator of computer or network malfunctions immediately.

Users must respect and protect the intellectual property of others by:

- Following copyright laws (not making illegal copies of music, games, or movies).
- Citing sources when using others' work (not plagiarizing).

Users must respect and practice the principles of community by:

- Communicating only in ways that are kind and respectful.
- Reporting threatening or discomforting materials to a teacher or administrator.
- Not intentionally accessing, transmitting, copying, or creating material that violates the school's code of conduct (such as messages/content that are pornographic, threatening, rude, discriminatory, or meant to harass).

- Not intentionally accessing, transmitting, copying, or creating material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works).
- Not using the resources to further other acts that are criminal or violate the school's code of conduct.
- Avoiding spam, chain letters, or other mass unsolicited mailings.
- Refraining from buying, selling, advertising, or otherwise conducting business, unless approved as a school project.
- Refraining from the use of social networking sites or applications such as Facebook, Twitter, Snap Chat or any other during school hours and/or when connected to a school network, unless directed by a classroom teacher or approved by an administrator.

Users may, if in accord with the policy above:

- Design and post web pages and other material from school resources.
- Communicate electronically via tools such as email, chat, text, or videoconferencing **(students require a teacher's permission)**
- Use the resources for any educational purpose.

Students may not use an audio recording device, video camera, or camera (or any device with one of these, e.g. mobile phone, laptop, tablet, etc.) to record media of any type, or take photos during school, unless they have permission from both a staff member and those whom they are recording.

8. Supervision and Monitoring

The use of digital devices at school is **not private**. School and network administrators monitor the use of information technology resources to help ensure that users are secure and in conformity with this policy. Administrators reserve the right to **examine**, **use** and **disclose** any data found on a student's device or the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions.
Minlaton District School reserves the right to determine which uses constitute acceptable use and to limit access to such uses.

Some examples of inappropriate activity on the Minlaton District School network that MDS reserves the right to take immediate action against may include (but is not limited to) activities *1) that create security and/or safety issues for the MDS network, Users, schools, network or computer resources; 2) that expend MDS resources on content it determines lacks legitimate educational content/purpose; or 3) other activities as determined by MDS as inappropriate.*
This includes (but is not limited to) examples such as:

- Violating any state or federal law such as: ○ Accessing or transmitting pornography of any kind, obscene depictions, harmful materials, materials that encourage others to violate the law, confidential information or copyrighted materials.
- Criminal activities that can be punished under law.
- Selling or purchasing illegal items or substances.
- Obtaining and/or using anonymous email sites, spamming, spreading viruses.
- Causing harm to others or damage to their property.
- Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
- Deleting, copying, modifying, or forging other Users' names, emails, files or data, disguising one's identity, impersonating other users, or sending anonymous email or messaging.

- Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance.
- Using websites, email, networks, or other technology for political uses or personal gain.
- MDS internet and intranet property must not be used for personal benefit.
- Intentionally accessing, creating, storing or transmitting material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others.
- Advertising, promoting non-MDS sites or commercial efforts and events.
- Breaching of copyright laws.
- Using devices or the network for non-academic related bandwidth activities such as games or transmission of large audio/video files or serving as a host for such activities.

9. Consequences of misuse

It must be noted that, if a student who is enrolled in a school, behaves online in a manner that threatens the wellbeing of a child, student, parent or member of the school community, even if this occurs off-site and/or out of school hours, the Principal has the authority under the Regulation pursuant to the *Education Act 1972* to suspend or exclude a student from attendance at school.

If the Principal suspects an electronic crime has been committed, this must be reported to the South Australian Police Department (SAPOL). Where there is a further reasonable suspicion that evidence of a crime, such as an assault, is committed on a mobile phone or other electronic device (e.g. a laptop or iPad), the device will be confiscated and handed to the investigating police officer. SAPOL will determine any further action.

If a student has circulated pornography it is a criminal offence. Police will be contacted by the school and a Suspension Pending Exclusion issued.

The electronic device in question will be secured in a plastic bag for collection by Police. No investigation will occur at a school level as it is a Police matter.

Violations of the standards outlined within this document may result in the following consequences, depending upon the violation:

- Discussion about incident with student(s) involved.
- Paying for excessive printing.
- Printer lockout.
- Internet lockout.
- Email lockout.
- Network (Computer) lockout.
- Completion of work without the assistance of the computer/device.
- Assuming financial responsibility for the repair, replacement or 'making right' of damage caused by the misuse of Minlaton District School property.
- Suspension from Learning Technologies activities.
- Suspension from school.
- Other disciplinary or legal action including the involvement of SAPOL.

10. Glossary of Terms

'Children and students' denotes all learners enrolled in DfE schools and preschools who are minors.

'Parent' used throughout this document refers to natural parents, legal guardians and caregivers.

'ICTs' in this document refers to 'information and communication technologies'.

'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. Examples include communications that seek to intimidate, control, manipulate, put down or humiliate the recipient.

'Digital footprints' are traces left behind by someone's activity in a digital environment. These traces can be analysed by a network manager or the police.

'Sexting' is where a person takes a sexually-explicit digital photograph of him or herself or of someone else, and sends it as an MMS and SMS via a mobile phone. These images can then be posted on the internet or forwarded electronically to other people. Once posted on the internet these images can leave a permanent digital footprint and be accessed at any time in the future. It is illegal to take sexual photos or videos of children and young people.

'Social networking' sites offer people new and varied ways to communicate via the Internet, whether through their computer or mobile phone. These sites allow people to easily and simply create their own online page or profile and to construct and display an online network of contacts, often called 'friends'. Users are able to build a network of connections that they can display as a list of friends. These friends may be offline actual friends or acquaintances, or people they know or have 'met' only online, and with whom they have no other link. Social networking sites are not limited to messaging, communicating and displaying networks. Nearly all sites allow users to post photos, video and often music on their profiles and share them with others.

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

'ICT equipment/devices', as used in this document, includes but is not limited to: computers (such as desktops, laptops, netbooks, 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' in this document 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. For examples of what constitutes an e-crime, please refer to the Cyber Bullying, E-crime and the Protection of Children parent brochure.

AGREEMENT FORM

It is a Department for Education (DfE) requirement that all students and their caregivers sign the *Acceptable Use of Learning Technologies Policy* before the student is permitted to access learning technologies on any Departmental site. Once signed and returned to school, the document is filed in the student's records and acknowledged in the school's database. This agreement then remains valid and in place for the duration of the student's enrolment at Minlaton District School or until it is reviewed or revoked by the school.

I have read and understood Minlaton District School's ***Digital Learning Policy*** and understand the ***Learning Technologies User Rights and Responsibilities*** within. I understand and accept the responsibilities outlined in this document.
I understand that this agreement remains valid and in place for the duration of my child's enrolment at Minlaton District School or until it is reviewed or revoked by the school.

Student Name	
Date of Birth	
Student Signature **YEAR 6-12 STUDENTS ONLY**	

Parent Name	
Parent Signature	
Date	