Technology: Student user family agreement

To enhance and complement the teaching and learning which happens at our site and to ensure our students can be successful global citizens in our ever-increasing technological world, our school aims to provide staff and students with the best technology equipment within our means. Students need to learn how to use technology respectfully and responsibly.

Information and signed agreements

There is a lot of information in this document so please take your time to read it thoroughly.

If you do not understand some aspects, please contact the school. Staff will go through this document with the students.

We would appreciate the signed agreements to be returned by the end of term 1 week 3 or earlier, so that your child can start accessing all technology available to them.

1. School and personal mobile devices

The term 'devices' includes items such as mobile phones, iPads, ipods, iwatches, smart watches with sims and tablets etc.

1.1 Primary and preschool students may use devices while traveling on the bus to and from school in a responsible and quiet manner.

1.2 Secondary students may use devices while traveling on the bus to and from school in a responsible and quiet manner.

No device is to be used at school from 9am – 3:20pm, devices must be off and away.

No devices, including laptops, are **not** to be taken or used in toilets, changerooms or the swimming pool area.

1.3 Students participating in excursions, camps or off-site supervised activities will be advised accordingly on the use of technological devices.

1.4 The school does not accept responsibility for theft, loss, damage, or health effects (potential or actual) resulting from any personal technological device. Damage of a school device needs to be reported to staff immediately.

2. Responsible and appropriate use of technology

2.1 **Photographs/ Recordings:**
Students have the right to be safe at school and a right to having their privacy being respected.
No photographs or recordings are to be taken of staff or other students on any device without their permission and they are definitely not to be shared online (text, email, internet based app, social media, etc.).

1

2.2 User IDs /passwords

Student passwords MUST be kept private. Any student found sharing their password, or any student caught using another student's password will have their network privileges suspended.

Passwords can be changed upon request if a student believes someone is misusing their credentials.

For their own security, students are advised to lock their computers when they are away from them.

2.3 Internet usage

An internet download quota is provided by the school and refreshed each term. Excess usage may be charged to the student.

Students are expected to restrict their internet use to study-related websites.

Internet use is directly monitored, and students will lose internet access privileges if they waste internet or access inappropriate material.

Social media websites are not to be accessed at school, and DECD has web filtering systems in place to prevent this.

2.4 Inappropriate use

- Accessing sites with content that is violent, racist, sexist, pornographic, dominated by offensive language and/or illegal in any way.
- Engaging in chat lines or downloading files not permitted, unless forming part of a legitimate class activity guided by the teacher of that class.
- Removing files or folders that have been installed to the hard disk or network.
- Using inappropriate or offensive names for files or folders. Please keep folder & file names to no more than 25 characters.
- Bringing to school, or use, games or any other materials which may be offensive to others.
- Engaging in cyber bullying or e-crime.

2. Monitoring user activity

While confidentiality and privacy is a high priority, the school reserves the right to monitor network and computer activity. This will involve monitoring of:

- Users computer screens
- Files in user's directories
- Files on portable storage devices or discs
- Internet activity
- E-mail
- General behaviour and respect for the computing resources throughout the site.

Staff can ask to view the laptop at school at any time.

3. Online safety/ Cyberbullying

Technology provides individuals with a powerful means of communicating instantly with others in both positive and negative ways. As students use technology at school and home, there is a need for a partnership between families and the school to support students to use practices to keep themselves safe online.

As part of the Child Protection Curriculum and Digital Technology Australian Curriculum, all students will learn about online safety and cyberbullying.

Information for families can be found at:
https://esafety.gov.au/
https://www.staysmartonline.gov.au/

https://bullyingnoway.gov.au/
https://au.reachout.com/everyday-issues/cyberbullying

4. For STUDENTS Year 4 and above: LearnLink Office 365

LearnLink Office 365 is a customised package of Microsoft Office 365 tailored for public schools and is offered at no charge to families while their student is at school.

The package provides students with an email address, Microsoft Office at home and school (up to 5 personal devices) and includes Word, Excel, PowerPoint, OneNote, Publisher and Outlook as well as other collaboration platform apps and 'cloud' storage. The applications can be used without an internet connection although a number of services provided by LearnLink Office 365 require internet access.

When students are at a school, internet access will be filtered by the Department for Education however, access from home/off-site is not filtered by the Department and as such should be supervised.

Please be aware that as with any internet use, it is possible (although unlikely) that viruses and/or other malicious software could be introduced to your personal computing devices via LearnLink Office 365 services (including email).

It is strongly recommended personal devices have suitable anti-virus / anti-malware software installed and regularly updated, and the device operating system is regularly updated.

Each student will receive 1 Terabyte (or 1000 Gigabytes) of storage space in Microsoft's Australian cloud. By default all data and files are private, however they can be shared with other LearnLink Office 365 users, including staff and students of other schools and preschools, but not anyone external to Department schools.

Users of LearnLink Office 365 are responsible for the information/data in their LearnLink Office 365 account and any important information should be backed up. The LearnLink Office 365 Service, is only to be used in relation to delivering curriculum objectives, **and will not be used to store sensitive or personal information.**
Staff will be using LearnLink Office 365, particularly in secondary school and students will be able to save work and access it from home online, which will be very useful.

Families need to give permission for their child's use of LearnLink Office 365.
If you wish to find out more information about LearnLink Office 365 or need help in downloading the applications at home, please contact the school.

5. For SECONDARY STUDENTS: School laptop and bag

The school is offering every secondary student a school laptop and bag for use at school and at home. It is preferred that students use the school laptop rather than their own. The laptop will be owned by the school.

5.1 Caring for your laptop
  It is an expectation that students will be responsible for the care of their school laptop. It is a privilege.
 • The laptops will have a school and home profile and will be identified with the student.
 • The laptop must be available for use at school each day and be fully charged.
 • As the laptop is the property of the school, it is not to be altered or personalised in any way eg. stickers or labels etc.
 • LCD screens are delicate – they don't like being poked, prodded, pushed or slammed. Never pick up your laptop by its screen. Don't slam the screen closed and always be gentle when putting your laptop down.
 • The laptop is not to be taken outside during recess or lunch time.

- The school must be notified immediately if the school laptop is lost, missing or damaged.
- Ensure the laptop is secure at all times; at school and at home.
- The device must be properly powered off prior to going in the bag to preserve battery life and to prevent heat build-up.
- Parents/caregivers will be liable to pay the replacement cost for wilful or accidental damage to the laptop.

5.2 Internet usage at home

Students may also use the internet for their personal use at home after setting up the device to access it through their home Internet Service Provider. However, students are reminded that inappropriate downloads can be detected when the devices are connected to the school's network. The school is not responsible for content filtering while at home, download usage and it is not responsible for ensuring compatibility with home internet connections.

5.3 Software, games, music, non-school applications

Non-school applications and files on the school laptops can be installed provided that the installed applications and files:

- Accessed through the home profile.
- Are appropriately licensed (i.e. they do not breach copyright and intellectual property laws – this includes video and music downloads)
- Are ethically and morally acceptable (including consideration of school appropriateness & are PG rated)
- Do not affect the efficient functioning of the laptops for educational purposes (i.e. they do not interfere with the speed and storage capacity of the laptop or the problems that might arise from increased battery use)
- Do not affect the school's wireless network
- Do not interfere with the learning program (i.e. they may only be used in class under specific teacher direction)
- The use of network games is banned
- No ad-hoc networks are to be formed.

5.4 Virus protection & regular updates

Anti-virus software and monitoring software will be loaded onto the device through the initial imaging process. Updates of this software may be scheduled at various times.
If a laptop attempts to connect to the school network and is found to have a virus, the student is required to tell the IT staff immediately.
Students should ensure that anti-virus software is kept up-to-date on their devices and regularly check for viruses. This can be done at no cost at the school.
As students have the right to personally use their laptops, and connect to the Internet from home, they need to take all steps to protect the laptop from virus attacks.

Viruses can enter laptops through:
1. Removable media such as CDs, DVDs and USB memory sticks
2. Emails
3. The internet (including web browsing, FTP programs and chat rooms)

TIPS
1. Do not open any files or links attached to suspicious or unknown emails.
2. Exercise caution when downloading files from the Internet. Save the files to the laptop's hard disk and run. the virus scanner on the files before opening them.
3. Delete chain and junk emails. Do not forward or reply to any of these.
4. Never reply to Spam.
5. Hundreds of viruses are discovered each month. Run your virus scan regularly.

5.5 Back up on network

It is always recommended to save curriculum work on the network at school as it is a more secure back up.

5.6 Technical support

Please contact the school IT manager it there are issues with the laptop.

5. For year 10-12 SENIOR SCHOOL STUDENTS: Personal laptops

It is preferred that students use the school laptop rather than their own due to reasons of security for the network and the availability of technical support. If year 10-12 students need to use their own due to specific reasons, permission is to be granted by the principal.

5.1 Requirements of personal laptops

The use of the laptop or device will be permitted as long as the user;

- explains the designated need to use the laptop,
- follows all of the user agreements as outlined in this document,
- installs the specific requirements of operating systems, anti-virus, java and adobe products as detailed by the IT Manager,
- has a home and school profile and only uses the school profile while at school,
- ensures there is no viewing or use of inappropriate content while at school,
- regularly updates the laptop,
- ensures the laptop has current electrical testing,
- fully charges the laptop at home and ensures it is available at school every day.

5.2 Technical support at school

It may be limited depending on the issues and hardware.

6. Consequences

Any student found to have breached any of the rules and expectations mentioned in this document, or behaving in an unacceptable manner with any of the technology facilities or equipment **depending on the severity and nature could;**

- immediately have their network account and/ or internet disabled for a period of time
- have their device confiscated for a period of time
- have a meeting with parent/ caregivers
- have a behaviour/ learning contract implemented
- have further relevant consequences
- in serious cases, be internally or externally suspended from school or involve SA Police.

Parents/ caregivers will be informed of any incidents.

Supporting documents

DECD Standard Acceptable Use Policies for Schools, Preschools and Children's Services' Sites
Cyber-safety -Keeping children safe in a Connected World

Technology: Parent/caregivers and student user agreement

Please detach, sign and return this agreement and keep the other information for future reference.

This agreement will cover the duration of your child's time at Karcultaby Area School.

Parent/ caregiver permission

☐ I have read and understand the information in the Technology: Student user agreement document. I understand that this form will be kept on file at school and that the details may be used and shared with a third party if necessary.

☐ I give permission for my child/ren to use their device/ school laptop as outlined in the agreement and understand that my child/ren will be responsible for ensuring the device/ school laptop is used appropriately and that consequences will result if the agreements are not followed.

☐ I understand that the school accepts no responsibility for replacing lost, stolen or damaged personal devices.

☐ **For students in year 4 and above**: I give permission for my child/ren to use LearnLink Office 365.

☐ **For secondary students:** I understand that we may be responsible for wilful or accidental damage to the school laptop.

Names of Students:	
Parent/caregiver name:	
Signature:	
Date:	