MOUNT COMPASS
AREA SCHOOL

ICT CYBERSAFETY ACCEPTABLE USE AGREEMENT

Government of South Australia
Department for Education

ICT USE AGREEMENT

1. We have read and understood this Cyber-safety Use Agreement and we are aware of the school's initiatives to maintain a cyber-safe learning environment.
2. We have read and understood the Bring Your Own Device, Electronic Communication, Learnlink Office 365 and Cloud Services Policies.
3. We understand our responsibilities regarding the use of the BYO device and the internet.
4. We understand that failure to comply will invoke the school's standard discipline procedures.
5. In signing below, we understand and agree to the above.

Name of student.:..... .... **Year** .... **Class**.............................

Signature of student... .... Date....................... ......

For the Parent/Caregiver/Legal Guardian: My responsibilities include…

- reading the ICT Cybersafety Acceptable Use, Bring Your Own Device, Electronic Communication, Learnlink Office 365 and Cloud Services Policies carefully and discussing them with my child so we both have a clear understanding of our roles in the school's work to maintain a cyber-safe environment
- ensuring this Use Agreement is signed by my child and by me and returned to the school
- encouraging my child to follow the cyber-safe strategies and instructions
- contacting the school if there is any aspect of this Use Agreement I would like to discuss
- understanding that MCAS strongly recommends the BYO device be covered by personal home and contents insurance.

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 DETACH & RETURN THIS SECTION TO SCHOOL AND KEEP THE AGREEMENT INFORMATION FOR YOUR OWN REFERENCE.

MOUNT COMPASS
AREA SCHOOL

ICT & CYBER-SAFETY USE AGREEMENT FOR MCAS STUDENTS

Government
of South Australia
Department for Education

ICT & CYBER-SAFETY AT MOUNT COMPASS AREA SCHOOL

Dear Parent/Caregiver,

The measures to ensure the cyber-safety of MCAS 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 Use Agreements for staff and students, who have been involved in the development of this 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 students.

The computer network, Internet access facilities, computers and other ICT equipment/devices bring great benefits to the teaching and learning programs at MCAS, 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 MCAS 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 students will be issued with a Use Agreement and once the signed consent has been returned to school, students 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. 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 is used to capture unsolicited or inappropriate images of students or 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 DE administrators to prevent student'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, DE cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. DE 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.

STRATEGIES TO HELP KEEP MOUNT COMPASS AREA 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. I will not use school ICT equipment until my parents/caregivers and I have signed my Use Agreement Form and the completed form has been returned to school.
2. 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.
3. I will keep my password private.
4. While at school or a school related activity, I will inform the teacher of any involvement with any ICT material or activity that might put me or anyone else at risk (eg bullying or harassing).
5. 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.
6. I will use my mobile phone/s only at the times agreed to by the school during the school day. (Please refer to the Electronic Communication Policy)
7. I will go online or use the Internet at school only when a teacher gives permission and an adult is present.
8. While at school, I will:
   - access, attempt to access, download, save and distribute only age appropriate and relevant material
   - not attempt to get around or bypass security, monitoring and filtering that is in place at school.
   - not damage computers, computer systems or networks. Furthermore, if I discover any methods of causing such damage I will report them to the network manager and I will not demonstrate them to others.
9. 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.

10. To ensure my compliance with copyright laws, I will download or copy files 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. Plagiarism is unacceptable. Therefore I will use any downloaded material in an appropriate manner in assignments, listing its source in a bibliography and clearly specifying any directly quoted material.

11. 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 the Use Agreement. Any images or material on such equipment/devices must be appropriate to the school environment.

12. Unless I have signed the ICT & Cybersafety Acceptable Use Agreement, only with written 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.

13. I will ask my teacher's permission before I put any personal information online. Personal identifying information includes any of the following (Please refer to the Cloud Services Policy):

- my full name
- my address
- my e-mail address
- my phone numbers
- photos of me and/or people close to me.

14. I will respect all school lCTs 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
- not to vandalise school equipment and software and to report any breakages/damage to a staff member.

15. 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.

16. 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.

17. 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.

INFORMATION FOR STUDENTS AND PARENTS

Printing

Each user is given an initial printing allocation. This allocation should be sufficient for their basic printing needs. Any user who exceeds this allocation is able to purchase extra printing credit through the Finance Officer. Users will be able to save paper (and money) by the following simple guidelines:

- Check work thoroughly before printing
- Use the Print Preview function
- When printing text from other sources (eg Internet), print only the required information
- Remember that colour printing costs 5c per page.

Unscheduled Use of Computers in Resource Centre or Computer Room

Students are permitted to use the Computer Room or Resource Centre only if there is a Staff member present. The following conditions apply to unscheduled access:

- Students must negotiate their absence from their regular class with their teacher and take a diary note to the Resource Centre/Computer Room.
- They must negotiate their presence in the Resource Centre/Computer Room; get their diary signed by the supervising staff member and fill out the 'Sign On' folder.
- If there is no one available (or prepared) to supervise, students must return immediately to their scheduled class.

LearnLink Office 365

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. LearnLink Office 365 including Office 365 ProPlus is only to be used in relation to delivering curriculum objectives, and must not be used to store, transmit or share sensitive or personal information.

For more information, please refer to the Learnlink Office 365 Policy and Cloud Services Policy which are available on our website.

I understand that MCAS will:

- endeavour 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 school ICT equipment/devices at school, or at school related activities; and enforcing the cyber-safety requirements detailed in Use Agreements
- respond to any breaches in an appropriate manner
- provide members of the school community with cyber-safety education designed to complement and support the Use Agreement initiative
- welcome enquiries at any time from parents/caregivers/legal guardians or students about cyber-safety issues.

For the Student:

My responsibilities include…

- reading this ICT & Cyber-safety Use Agreement carefully
- following the cyber-safety strategies and instructions whenever I use the school's ICTs
- following the cyber-safety strategies whenever I use privately-owned ICT devices on the school site or at any school related activity, regardless of its location
- avoiding any involvement with material or activities that could put at risk my own safety, or the privacy, safety or security of the school or other members of the school community
- taking proper care of school ICTs. I know that if I have been involved in the damage, loss or theft of ICT equipment/devices, I and/or my family may have responsibility for the cost of repairs or replacement
- keeping this document somewhere safe so I can refer to it in the future
- asking the School if I am not sure about anything to do with this agreement.

Consequences of unacceptable use

Unacceptable use of information and communication technologies (ICTs) at MCAS could result in the following action regardless of the student's area of study.

- A behaviour management form will be completed
- Student will be referred to the management staff
- Student privileges related to the use of information technology will be suspended for a period of time determined by the management staff.

BRING YOUR OWN DEVICE (BYOD) POLICY

(to be reviewed in 2021)

BYOD refers to technology models where students bring and use their own personal digital device to school for the purpose of learning.

Mount Compass Area School has invested significant funds in upgrading and supplying state of the art ICT network infrastructure. We have funded and built a progressive, modern 'digital highway' to make sure your child gets access to the best learning opportunities available. Students in this modern learning environment require a device they can use at home and school. Therefore, we are seeking your assistance by asking you to provide your child with an appropriate personal ICT device so that they can connect to this network which will enhance their engagement and learning.

To support us in delivering this initiative we have developed a BYOD Policy with standards and guidelines to;

- enable and promote bringing a suitable computing device to school by all students for use in their education
- provide a safe user environment for students
- ensure a minimum standard of device compatibility
- enable students to use technology to further their learning, independently and in structured lessons
- provide a basis on which Mount Compass Area School teaching staff can continue to tailor lesson delivery so that students can use their devices in class toward specific learning outcomes.

Students and Parents

- It is essential that students embrace new learning technologies with the expectation that all Year 7 and 10 students will bring a suitable computing device to school each day.
- Year 6 students are strongly encouraged to bring a suitable computing device to school each day.
- There are significant learning advantages in Upper Junior, Middle and Senior School students having their own personal and compliant computing device
- Should a student acquire a personal computing device at the end of Junior School/beginning of Middle School it is recommended that this device be upgraded at Year 10 to support the student through their final years of schooling and into work or future study
- It is strongly recommended that by Year 10 every student will have their own computing device to ensure full and uninterrupted participation in the learning opportunities
- The personal device must be available to be brought to school each and every school day and be solely for the student to use throughout the day.

Staff

- Teachers will encourage and facilitate the use of students' devices in their classes where they deem appropriate. Use of students' own devices in class is, however, at the sole discretion of the teacher
- Staff will not allow any devices to be charged at the school.

Students and parents are responsible for ensuring the device brought to school meets all the requirements of the **Bring You Own Device - Minimum device specifications and considerations** documentation

- **Device Specifications** - A device which does not meet the specifications will not be permitted to access the school network and services
- Prior to bringing a personal device for the first time, students and their parents must read and sign the **ICT Cybersafety Acceptable Use Policy**
- Students must use their device in accordance with the school's **ICT Cybersafety Acceptable Use Policy** and this **BYOD Policy**
- Students will follow teachers' directions as to appropriate use of their devices in class.
- Each student is absolutely and solely responsible for the care and conduct of his / her own personal device whilst at school and travelling to and from school.
- Parents and student should consider whether their device requires insurance and whether specific accidental loss and breakage insurance is appropriate for the device
- Students must connect their device to the designated wireless data network supplied by Mount Compass Area School using their own credentials only
- Students must not connect to any other network, wired, wireless or cellular whilst at Mount Compass Area School
- Students must not bridge the School's designated network to any other network
- Due to DfE Work Health and Safety restrictions, **students must bring their device to school fully charged** and should not bring any power chargers and cables to school with their device
- Voice, video and image capture applications may only be used with teacher permission and relevant to the learning environment whilst being respectful of the rights of others.

Mount Compass Area School will:

- Promote bringing of a computing device to school by all Year 6-12 students by ensuring the device specifications are designed so that a range of devices in capability and cost are suitable
- Ensure all Year 6-12 students have access to technological resources in their required classes by maintaining a base set of laptops and computers for students who cannot access the BYOD program
- Provide a BYOD Policy to list the responsibilities and expectations of each student and their families in the BYOD program
- Ensure a copy of the **BYOD User Agreement** is signed by each student and their parents prior to allowing the student's device to be brought to school
- Publish a Device Specification code that describes the requirements for devices brought to school.
- Provide a wireless network with filtered internet connection to which students may connect their BYOD program device
- Provide initial support to assist students with first bringing their device to school and establishing network connectivity
- The Department for Education does not provide insurance for accidental loss or damage to devices brought to schools for use by students. However, claims may be met under the department's public liability insurance where the loss or damage is attributable to a negligent act or omission on the part of the school.
- Should a student's device fail to meet a requirement of the Device Specification, the school will not facilitate the student access to any network or school services.

MOUNT COMPASS
AREA SCHOOL

BYOD MINIMUM DEVICE SPECIFICATIONS

Government of South Australia
Department for Education

Minimum device specifications and considerations

Families wishing to purchase a device supporting our BYOD Policy need to refer carefully to the following **Device Specifications:**

While all devices meet the minimum system requirements/hardware specifications, the school strongly recommends that students **choose a laptop device or tablet with keyboard** to ensure that their BYOD maximises their experience.

- **Screen size** - MUST be 10" or bigger. Students spend a large part of their school time & home study interacting with the device, so a large, clear screen is important
- **Battery life** –It is expected that the device is fully charged at the start of every day. There is **NO option to charge these devices at school**. Please choose devices with at least 6 hours of battery life.
- **RAM –** The speed of the device is determined in part by the amount of memory it has. We recommend 4GB RAM for notebook-style devices.
- **Operating System** – Microsoft Windows 8.1 or newer,

  Microsoft Windows 10 Home
  Windows 10 version "S" will complicate connecting to our network resources and is strongly advised against. It can be upgraded for free to Windows 10 Home.

  Apple MacOS 10.8 or newer,

  IOS 7 or newer

- **Wireless compatibility** – Device must have 5Ghz 802.11n support, which may be advertised as Dual Band Wireless, 802.11abgn, 802.11agn, 801.11ac or Gigabit Wireless
- **Weight** - Please be aware of the weight of a device when purchasing, as there is potential for user discomfort
- **Durability** - You will need to consider the durability of the device, as your child will be carrying it to and from school as well as from class to class
- **Antivirus** - Students must have an anti-virus program installed on their device, and are required to keep it updated.
- **External hard drive** (*recommended*) - to backup files on a frequent basis. This ensures that documents (including school work) are backed up to an external device.

MOUNT COMPASS
AREA SCHOOL

PO Box 54, Mount Compass SA 5210
T (08) 8556 8219
F (08) 8556 8471
E dl.0289_info@schools.sa.edu.au
www.compassas.sa.edu.au

Primary student use of mobile phones and personal devices

Purpose

This policy provides direction to students, staff and families about managing mobile phones and other digital devices that students choose to bring to school. Digital devices include, but are not limited to, smartwatches, tablets or laptops that are not part of a separate Bring Your Own Device arrangement. This policy applies while students are at school, or attending an authorised school activity such as an excursion, during school hours.

Mobile phone use for primary school students
The department's position is that primary aged students cannot use their mobile phones and personal devices at school during school hours. The department and the school recognise that there are legitimate reasons for students to bring a mobile phone or personal device to school. This may include:

- to ensure their safety while travelling
- so that parents can contact them outside of school hours.

During the school day, students are not permitted to access or use their mobile phones or other personal devices. Students must switch off or mute their devices before storing them at the beginning of the school day. They will not be able to access their device until the end of the school day.

Storage of personal devices

Students' personal devices will be stored in their bag for the duration of the school day. Students who are distrustful of this approach may have their devices signed in at the front office. Students/parents are able to negotiate the storage of their device to be delivered to the front office prior to lesson 1 and collected at the end of the school day.

If the student does not comply Consequence for a breach of the policy:

- First Offence – phone/device removed by teacher and placed at the front office for collection at the end of the day; parents notified of this occurrence
- Second Offence – phone/device placed in front office to be collected by parent; student receives one day external suspension
- Third Offence – external suspension for up to three days

Roles and responsibilities

Principal

Make sure:

- this policy is clearly communicated and accessible to all students, staff, and families
- there is a process for regular review of the policy
- secure storage is provided for student personal devices that are handed in to school staff and individual lockers or locks that the school provides for students to store their belongings are appropriately secure
- processes are in place for monitoring internet and school network use by all members of the school community.

Enforce the policy and responses to instances of non-compliance.
Report and respond to incidents of inappropriate use of personal devices in line with department policy and procedures and any legislative requirements.
Model appropriate use of mobile phones and support families to understand the importance of promoting safe, responsible and respectful use of mobile phones to their children.

School staff

Deliver learning opportunities and maintain a safe and productive learning environment. Take steps to minimise distractions from the non-educational use of personal devices in the learning environment.
Respond to instances of non-compliance in line with the school's policy.
Report and respond to incidents of inappropriate use of personal devices in line with department policy and procedures and any legislative requirements.
Model appropriate use of mobile phones and support families to understand the importance of promoting safe, responsible and respectful use of mobile phones to their children.

Students

Comply with the requirements of the school's policy, and follow all reasonable directions from the Principal and school staff.
Respect others' rights to privacy and do not take photos, film or audio records of other people without their knowledge or permission.

Parents

Support the implementation of the school's policy, including the consequences for non-compliance with the policy.
Use the school's formal communication channels in all instances to communicate with the school (including where a student requires early collection from school). Encourage their child to always report to a school staff member in the first instance if they become unwell or experience an issue at school.
Recognise the important role they play in supporting their child to use their mobile phone (or other personal device) in a safe, responsible and respectful way.

Communication and review

- Information shared in communication titled *The social discourse created by social media* which outlined our school approach based on international research
- Governing Council supported this action, policy and process
- Student leaders consulted annually regarding the policy
- All school policies are reviewed every third year
- Policy is located at J/Staffshare/Policy and Procedure/Operations

Secondary student use of mobile phones and personal devices

Purpose

This policy provides direction to students, staff and families about managing personal mobile phones and other digital devices that students choose to bring to school. Digital devices include, but are not limited to, smartwatches, tablets or laptops that are not part of a separate Bring Your Own Device arrangement. This policy applies while students are at school, or attending an authorised school activity such as an excursion, during school hours.

Mobile phone use for secondary school students

Our school recognises that there are legitimate reasons for students to bring a mobile phone or personal device to school. This may include:

- to ensure their safety while travelling
- so that parents can contact them outside of school hours.

Year 7 to 10 students are not permitted to use mobile phones or devices during the school day that are not part of our Bring Your Own Device arrangement.

Year 11 and 12 students are permitted to use mobile phones discretely during break-times but not during lesson times unless the use is for learning purposes and is firstly negotiated with the teacher.

Storage of personal devices

Mobile phones and other devices are to remain in the student's bag during school hours.

If the student does not comply

- First Offence – phone/device removed by teacher and placed at the front office for collection at the end of the day; parents notified of this occurrence
- Second Offence – phone/device placed in front office to be collected by parent; student receives one day external suspension
- Third Offence – external suspension for up to three days

Internet connection for personal devices

Students are permitted to use electronic devices for the purpose of learning as outlined in the schools *Electronic Communication Policy.* Connection to the school's ICT network is via wifi however, students are not permitted to charge their personal devices at school.

Roles and responsibilities

Principal

Ensure:

- this policy is clearly communicated and accessible to all students, staff and families
- there is a process for regular review of the policy
- secure storage is provided for student personal devices that are handed in to school staff and individual lockers or locks that the school provides for students to store their belongings are appropriately secure
- processes are in place for monitoring internet and school network use by all members of the school community.

Enforce the school's policy and responses to instances of non-compliance.
Report and respond to incidents of inappropriate use of personal devices in line with department policy and procedures and any legislative requirements.
Consider requests for exemptions from the school policy from parents, adult or independent students on a case-by-case basis. Make sure that approved exemptions are documented and that relevant staff are informed about students' exemptions.
Model appropriate use of mobile phones and support families to understand the importance of promoting safe, responsible and respectful use of mobile phones to their children.

School staff

Deliver learning opportunities and maintain a safe and productive learning environment. Take steps to minimise distractions from the non-educational use of personal devices in the learning environment.
Respond to instances of non-compliance in line with the school's policy.
Report and respond to incidents of inappropriate use of personal devices in line with department policy and procedures and any legislative requirements.
Make sure that any student personal devices handed in for their care are stored in a secure location and are returned to the student (or their parent).
Model appropriate use of mobile phones and support families to understand the importance of promoting safe, responsible and respectful use of mobile phones to their children.
Familiarise students with the option of accessing a BYOD locker for security purposes.

Students

Comply with the requirements of the school's policy, and follow all reasonable directions from the Principal and school staff.
If permitted to use a mobile phone or personal device in line with this policy, do so in a safe, responsible and respectful way and support peers to do the same.
Communicate respectfully with others and do not use a mobile phone or other personal device to bully, harass or threaten another person.
Respect others' rights to privacy and do not take photos, film or audio records of other people without their knowledge or permission.

Parents
Support the implementation of the school's policy, including the consequences for non-compliance with the policy.
Use the school's formal communication channels in all instances to communicate with the school (including where a student requires early collection from school). Encourage their child to always report to a school staff member in the first instance if they become unwell or experience an issue at school.
Recognise the important role they play in supporting their child to use their mobile phone (or other personal device) in a safe, responsible and respectful way.

Communication and review

- Information shared in communication titled *The social discourse created by social media* which outlined our school approach based on international research
- Governing Council supported this action, policy and process
- Student leaders consulted annually regarding the policy
- All school policies are reviewed every third year
- Policy is located at J/Staffshare/Policy and Procedure/Operations

MOUNT COMPASS
AREA SCHOOL

CLOUD SERVICES POLICY

Government
of South Australia
Department for Education

What are Cloud Services?

Cloud Services are provided by many different companies and vendors that provide you email and/or collaboration platforms to create and/or upload/share content. This includes websites, presentations, written, audio, images and video material as part of your educational program.

Data and information within the cloud could be stored anywhere in the world and can be covered by various privacy laws. Mount Compass Area School (MCAS) performs thorough risk analysis before approving the use of any online cloud service.

Using Cloud Services

You are required to sign conditions of use agreements before you have access to school computers, internet, and software which outlines acceptable use.

Cloud services require internet access and when you are at school internet access will be filtered by the Department for Education (DE) however access from home/off-site is not filtered by DE and as such, students should be supervised.

Please be aware that as with any internet use, it is possible that viruses and/or other malicious software could be introduced to your personal computing devices via cloud 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.

You are responsible for the information/data in any of your personal cloud accounts and any important information should be backed up. Cloud services are only to be used in relation to delivering curriculum objectives, and must not be used to store, transmit or share sensitive or personal information.

Installing Cloud applications

Some cloud services can be installed as applications.

It is possible that installing cloud applications on your personal device may cause problems, such as conflicts with other software you have installed.

It is recommended that you:

- Backup your personal device, prior to installing applications; and
- Ensure your personal device meets or exceeds the requirements for that particular application.

What if I do not want my child(ren) to use the Cloud Services?

Mount Compass Area School requires written notification if you do not consent to your child(ren) using Cloud Services.

Please use dl.0289.info@schools.sa.edu.au to notify the school.

Additional reading

The information and link provide additional information about keeping children safe online:

- Appendix A: Student privacy and information summary
- Cyber-safety, bullying and harassment

https://www.education.sa.gov.au/supporting-students/health-e-safety-and-wellbeing/cyber-safety-bullying-and-harassment

Appendix A: Student privacy information summary

Information/data storage location:

MCAS will ensure that any information/data for approved cloud services is stored in Australian data centres and is subject to Australian Privacy Laws, regulations, and standards.

If the information/data is stored off-shore, MCAS will ensure the privacy laws, regulations and standards are comparable to those of Australia.

When the information/data is stored off-shore and is not covered by comparable privacy laws, regulations or standards, MCAS will to the best of our abilities, restrict the uploading of confidential and/or identifiable information or will not approve use of that service.

Cloud service data collection:

Cloud service data collection requirements vary for each service/company. MCAS will ensure only the minimum amount of data/information required by the approved cloud service is provided and will restrict providing confidential or identifiable information to those approved cloud services covered by Australian privacy laws, regulations and standards.

Learning materials used by educators to teach the student, and information/data created or uploaded by the student in the approved cloud service will be stored in their data centres. This may include text, images, photographs, sound and multimedia (e.g. videos).

Cloud services have varying policies regarding the access, use, tracking or collecting of information or data about the users/student. MCAS will ensure that approved cloud services are covered by Australian privacy laws, regulations and standards.

Access to my child's information and data:

Cloud service data access varies depending on the service. MCAS will ensure that any approved cloud services will not on-sell information and data to any third-parties and that the user/student owns and controls the information and data they create or upload. MCAS will also ensure that users/students can only share (if allowed to do so) their information and data with others at MCAS and/or staff and students from within DE schools or preschools. MCAS will ensure anyone external to DE is unable to access confidential and/or identifiable student information.

Processes are in place to allow authorised DE staff to access information and data the student has created or to uploaded to some services (such as Office 365 and OneDrive) where required.

MCAS will ensure that any approved cloud services will only disclose information if required to do so by law.

Safety of the student's information and data:

MCAS will ensure any approved cloud services where confidential and/or identifiable information is provided are certified by the Australian Government as safe to use for government information. MCAS will also ensure approved cloud services meet international security standards.

MOUNT COMPASS
AREA SCHOOL

Learnlink Office 365 Policy

Government of South Australia
Department for Education

What is LearnLink Office 365?

LearnLink Office 365 provides you an email and collaboration platform to create and/or upload/share content. This may include websites, presentations, written, audio, images and video material as part of your educational program.

All data and information within LearnLink Office 365 is stored within an Australian based 'cloud' and provides the following services.

- **Email**
  You are provided a unique email address that remains the same throughout your enrolment in a State Government school or preschool.

- **Office 365 ProPlus**
  Office 365 ProPlus provides the latest versions of Microsoft Office applications for desktop PCs, Macs and mobile devices, including Windows, iOS and Android devices.

  Office applications include Word, Excel, PowerPoint, OneNote, Access, Publisher and Outlook, however not all Office applications are available for Mac, iOS and Android devices.

  Office applications can be installed, via the internet, on up to 5 personal computers and up to 5 mobile devices owned by you (or parent-owned). Once installed, the applications can be used without an internet connection. Periodic internet connection is required for accessing data stored in cloud services, updates and licencing via your LearnLink Office 365 account.

- **Office Online**
  Office Online is a web based, lightweight version of Microsoft's Office productivity suite (including Word, PowerPoint, Excel, and OneNote) that can be used on most devices capable of connecting to the internet via a web browser.

- **OneDrive for Business**
  OneDrive for Business is a cloud service where you can store, sync, update, and share files from any internet connected web-browser, and collaborate on Office documents.

  You 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 the Department for Education (DE) schools/preschools.

Using LearnLink Office 365 Services

You are required to sign conditions of use agreements before you have access to school computers, internet, and software which outlines acceptable use.

A number of services provided by LearnLink Office 365 require internet access.

When you are at a school internet access will be filtered by DE however access from home/off-site is not filtered by DE and as such, students 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.

You are responsible for the information/data in your LearnLink Office 365 account and any important information should be backed up. LearnLink Office 365 including Office 365 ProPlus is only to be used in relation to delivering curriculum objectives, and must not be used to store, transmit or share sensitive or personal information.

Installing Office 365 ProPlus

Office 365 ProPlus applications will need to be installed on a computer or mobile device (personal device) before it can be used.

Although unlikely, it is possible that installing Office 365 ProPlus on your personal device may cause problems, such as conflicts with other software you have installed.

It is recommended that you:

- Backup your personal device, prior to installing Office 365 ProPlus application(s); and
- Ensure your personal device meets or exceeds the Office 365 System Requirements https://products.office.com/en-au/office-system-requirements.

What if I do not want my child(ren) to use the LearnLink Office 365 Services?

Mount Compass Area School requires written notification if you do not consent to your child(ren) using the additional LearnLink Office 365 Services.

Please use dl.0289.info@schools.sa.edu.au to notify the school.

How will I access the LearnLink Office 365 Services?

LearnLink Office 365 services can be accessed by logging into the DE LearnLink student portal http://www.learnlink.sa.edu.au.

Additional reading

The information and link provide additional information about keeping children safe online:

- Appendix A: Office 365 student privacy and information summary

- DE Cyber-safety: Keeping Children Safe in a Connected World
  http://www.DE.sa.gov.au/docs/documents/1/CyberSafetyKeepingChildre.pdf

Appendix A: Office 365 student privacy information summary

Where will the information/data be located?

LearnLink Office 365 service is a Cloud based service, meaning it can be accessed from any Office 365 compatible internet connected device anywhere/anytime. All the information and data is stored in Microsoft's Australian data centres and is subject to Australian Privacy Laws, regulations, and standards.

What information and data will be collected?

Learning materials used by educators to teach the student, and information/data created or uploaded by the student in the LearnLink Office 365 service will be stored in the data centres. This may include text, images, photographs, sound and multimedia (e.g. videos).

Microsoft does not access, use, track or collect information or data about the student, other than to deliver the Office 365 service on behalf of DE. In doing so, some system generated data is logged, such as who accessed the services and when.

Who has access to my child's information and data?

The student owns and controls the information and data they create or upload to the LearnLink Office 365 service. They can share their information and data with other LearnLink Office 365 users; this includes staff and students from other DE schools or preschools. Anyone external to DE is unable to access student information and data.

Processes are in place to allow authorised DE staff to access information and data the student has created or to uploaded to the service where required.

Microsoft will only disclose information and data at the direction of DE or if required to do so by law.

How safe is the student's information and data?

Microsoft's Office 365 Service (LearnLink Office 365) has been certified by the Australian Government as safe to use for government information. The certification letter and report has been verified by DE. Additionally Microsoft's Office 365 Service is certified to several international security standards.