COMMUNITY
VISION
ACHIEVEMENT
INNOVATION

ICT USER AGREEMENT

"At MOC we believe the future is now in education
& we must deliver on that brief"

Mark Oliphant College

All Department for Education schools and preschools are provided with internet access, Cyber-safety of Mark Oliphant College is based on our core values.

(08) 8209 1600 info@moc.sa.edu.au www.moc.sa.edu.au

Government of South Australia
Department for Education

CONTENTS

INTRODUCTION

Dear Parent/Caregiver,

The measures to ensure the cyber-safety of Mark Oliphant College 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 User Agreement Form.

Rigorous cyber-safety practices are in place, which include cyber-safety User Agreement s for staff and students, 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 students.

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

This document will act as the User Agreement and once signed and returned to the school, students will be able to use the school ICT equipment.

Material sent and received using the network may be monitored; 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 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 the Department for Education 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, the Department for Education cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. The Department for Education 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 school, if you have any concerns about your child's safety in using the Internet and ICT equipment/devices.

Any references within this document to the term 'user' will encompass any person or persons accessing ICT resources of Mark Oliphant College.

DEVICES

Devices are issued to the user for educational use and remains the property of Mark Oliphant College and the supply of a device to the user is conditional upon the user's continued association with the College and ongoing agreement to the terms of usage.

If the student ceases enrolment at Mark Oliphant College, the device must be returned to the College on the date we specify by notice to you, or on the date the student ceases to be enrolled at Mark Oliphant College, whichever is earlier, you must return the laptop to Mark Oliphant College in good working order and in good repair and if applicable, complete with the AC power adaptor.

Failure to return the device in its original condition will result in Mark Oliphant College invoicing the student or parents/carers for the repair or replacement cost of the device.

- The device may not be used for any commercial purposes
- This agreement is only valid in Australia. The device cannot be taken on holiday overseas
- Each student issued with a device is expected to care for and safeguard the device in a responsible manner. The device is an expensive item of College property and the College issues this property to the student on the understanding that it will be well cared for.
- The type of provided device is determined at the discretion of Mark Oliphant College based on determining factors such as year level and educational purpose.
- A Device may reference an iPad, iPod, iMac, Macbook, Laptop, Desktop, Chromebook, or any other digital device provided by Mark Oliphant College or used whilst onsite
- Mark Oliphant College does not give any warranty, representation or assurance as to the quality, fitness for purpose or safety of the iPad as this is covered by the Manufacturer.
- All material on devices is subject to review by College staff.
- Devices owned by Mark Oliphant College periodically check in to report configuration and management information, the information in these reports may contain but not be limited to the following: Internet provider information, Geographical location, IP Address details, installed applications and their usage, Disk Usage, Plugged in or synchronised devices, battery status, hardware information and internet activity.
- The security and use of the device is the student's responsibility. The student must comply with all directions the College and its staff give in relation to the use of the device and produce the device for inspection whenever requested.
- A device is permitted for personal use provided this use does not affect the performance of the device.
- All material on the device is subject to review by College staff and must meet all acceptable use criteria.
- Mark Oliphant College may lock or disable the device at any time
- Students are not permitted to change device specifications, make modifications, add upgrades, or attempt to access the device internals.

APPEARANCE AND PERSONALISATION

- As the devices are the property of the College, the appearance of the laptop must not be changed in any way. The barcode and serial number must not be defaced and the entire device must remain clear of any additional stickers, signage or graffiti.
- The iPad will be permanently marked with identifying information as required by the Administrative Instructions & Guidelines (AIGs). Additionally, a label containing the Asset Tag Number will be attached. This label must not be removed.

CLEANING

- To clean your device or its screen:
    - Switch off your device
    - Lightly dampen a non-abrasive cloth with water and gently wipe the screen in a circular motion.
    - Use a microfiber cloth to gently dry off any remaining residue
- Do not directly apply water or cleaner to the device or its screen

LOSS AND DAMAGE

- Warranty on devices covers normal defects and usage issues. It does not cover negligence, misuse, abuse, malicious act or loss.
- It is the student's responsibility to take appropriate precautions to prevent wilful damage or theft.
- In the case of loss or damage as a result of negligence, abuse or malicious act the student or the parents/carers will be responsible for meeting the cost for repairs or full replacement of the device.
- Device screens are delicate and will be damaged if poked, prodded, pushed or slammed
- Any instances of vandalism, damage, loss or theft must be reported immediately to the College. In the case of a suspected theft a police report must be made by the family and an event number provided to the College.
- Parents/carers will have to replace lost or damaged chargers.
- Students are not to deface any College device or part thereof.
- The student or their family must not try or purport to sell any College device, offer the device as security nor give possession of the device to anyone else.
- Parents may choose to evaluate their personal home contents and car insurance to cover equipment on loan to their child in the event of loss or damage to such loaned equipment while in the care and custody of the child.
- In instances where damage or loss has occurred involving students other than the student it has been assigned to, the incident will be further investigated.
- In the case of accidental loss or damage a witnessed statutory declaration signed by the parent/carer should be provided
- If a device is damaged or lost the college will determine whether replacement is appropriate and/or whether or not a student retains access for home use if applicable

POWER ISSUES/BATTERY/CHARGING

- The battery can be conditioned to ensure a long life.
    - The device battery should be completely powered down before recharging
    - It should then be fully charged whilst the device is powered off
    - Use the device without recharging until it powers itself off
    - Repeat this process 2 times
- Devices can be used with the AC charger attached where power sockets are safely available
- Students able to take the device home must bring the device to the College fully charged each day. Classrooms may have limited facilities to recharge devices.

SECURITY PROCEDURES

- Do not leave your device logged-on when you are not using it. It is strongly recommended that you secure your device with a password protected screensaver or pin code. This locks your device after a set period of inactivity, reducing the risk of someone else performing any actions using your digital identity.
- You must update software with security patches when they are released. This occurs automatically whenever your laptop is connected to the College network, notifications may offer early adoption of required updates.
- During the College day when the devices are not being used and the student is unable to keep the laptop on them (e.g. at lunchtime, during PE etc), the devices should be securely stored in the classroom or designated storage area.

DATA RESPONSIBILITY

- Information stored ON the device is not backed up by ICT systems
- Mark Oliphant College provides network and cloud storage facilities for daily use and or backup locations, network storage is regularly backed up by the College
- In the event of failure, our College IT technician(s) may be able to restore your device to its original state. There is no guarantee that data stored on your device can be recovered. Before installing new software, ask first for assurance and make sure your backups are up to date.

SOFTWARE, COPYRIGHT, AND INTELLECTUAL PROPERTY

- Each device will be loaded with a Mark Oliphant College approved software image configured for use on the College network.
- Where applicable the image will include anti-virus software, Microsoft, Apple, and Google software
- Software installed by the College is copyright and must not be distributed or deleted without written permission from the College.
- Mark Oliphant College does not object to the installation of non-College applications and files on the College laptops provided that the installed applications and files:
    - 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 College appropriateness, age-appropriate ratings, and privacy issues)
    - Do not interfere with 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 interfere with the College's wireless network
    - Do not interfere with the learning program.
- While some games have significant educational benefits, other games have little educational merit and may affect network function. As a result:
    - The use of non-College supplied network games is banned
    - No ad-hoc networks are to be formed.

CARING FOR YOUR DEVICE

- For extra protection, always pack your device in a protective cover if you are carrying it from one place to another or in your College bag.
- Do not remove a cover from an iPad unless directed to do so
- Do not wrap the cord too tightly around the power adapter or the cord will become damaged
- You still need to be careful with a device whilst it is in your bag. Do not drop the bag from your shoulder. Always place the bag gently down.
- Laptops should be switched off before being placed into a protective cover.
- Avoid exposing your device to:
    - Direct sunlight or sources of heat such as desk lamps
    - Dust, dirt, rain, liquids, or moisture
    - Heavy shock or vibration.
    - Avoid applying pressure to the screen of any device
    - Do not store your device in the vicinity of a water bottle or container holding liquid

VIRUS PROTECTION

For applicable devices the following applies

- Anti-virus software (McAfee or Microsoft) and monitoring software will be loaded onto the device through the initial imaging process. Updates of this software may be scheduled at various times.
- Students should ensure that anti-virus software is kept up to date on their laptop and regularly check for viruses.
- Internet traffic is automatically scanned for viruses when connected to the College network.
- Students that have the right to personally use their device and connect to the Internet from home are required to take all steps to protect the device from virus attacks.
- You must not install any additional antivirus software as this can cause conflict with existing Antivirus software
- Viruses can enter laptops through:
    - Removable media such as CDs, DVDs, and USB memory sticks
    - E-mails
    - The Internet (including web browsing, FTP/Torrent programs and chat programs/rooms).
- Helpful TIPS
    - Do not open any files attached to suspicious or unknown emails
    - 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
    - Delete chain and junk emails. Do not forward or reply to any of these
    - Never reply to Spam
    - Hundreds of viruses are discovered each month. Run your virus scan regularly
    - Avoid indiscriminately loading non-standard software onto the laptop as it can result in an infection by viruses and spyware which are a common cause of laptop failure.

ACCEPTABLE USE

The ICT Network Managers maintain devices and network infrastructure so that they operate effectively, ensuring that the resources needed are available for all users, and that the network operates in an even and consistent way. The following guidelines are outlined to ensure all users are able to access the latest research available with the latest technology in an acceptable and safe learning environment.

- Users will avoid 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 is not permitted unless forming part of a legitimate class activity guided by the teacher of that class
- The Federal Communications Act determines guidelines for appropriate use. Inappropriate use of the internet and email is a serious matter and can have significant consequences, e.g., sending a message over the internet using someone else's name.
- It is the responsibility of students to maintain sufficient credit in their printing accounts to allow subject related tasks to be carried out.
- Do not name files, folders, aliases, or applications inappropriately with content that is violent, racist, sexist, sexual, or provocative.
- Do not engage in cyber bullying or e-crime
- Passwords should remain confidential. No user should log-on another student using their password
- Do not bring into the College, or use, games or any other materials which may be offensive to others
- No device with camera capabilities is to be used in change rooms or toilets
- Under privacy legislation it is an offence to take photographs of individuals without their expressed permission and place these images on the Internet or in the public forum
- Circumvention, bypassing or disabling of monitoring, recording or administrative systems is prohibited. Some of these systems or services may include but not be limited to; proxy bypass technologies, VPN/TOR networks, websites designed to download content from filtered websites
- Circumvention of, or disconnection from, the Mark Oliphant College WiFi service whilst on site is prohibited, this includes ‘hotspotting’
- Any privately owned / personal device brought to Mark Oliphant College is also subject to the ICT User Agreement

CYBER BULLYING

E-technology provides individuals with a powerful means of communicating instantly with others in both positive and negative ways.

By Definition 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 email, chat room discussion groups, instant messaging, WebPages or SMS (text messaging)–with the intention of harming another person

Examples of cyber bullying include but are not limited to, communications that seek to intimidate, control, manipulate, put down or humiliate the recipient.

Any form of cyber bullying or e-crime will be dealt with through the College’s “Harassment Policy” and “Acceptable Use of Technology Policy”.

Serious breaches are a police matter and will be dealt with through State & Federal laws and SA police.

INTERNET USE

- Users can access the Internet through the College's network while on site. Access to the Internet through the College's network will be monitored and subject to strict filtering.
- Attempts to bypass internet filtering or access illegal services will result in a temporary ban of internet services. Filtering is setup to automatically apply bans as soon as circumvention methods are detected.
- Torrent and unapproved VPN traffic detected on the College network is prohibited
- Users are responsible for the content that their internet account accesses.
- Users are to only connect to the internet using their own user account
- All internet access on the College's network is recorded and logged outside of the device
- Offsite internet usage of the school provided device may be recorded
- Mark Oliphant College is not responsible for any materials viewed on networks that are foreign and or external
- Mark Oliphant College is not responsible for any data charges incurred by the use of a supplied device on networks that are not provided by the College.

EMAIL & SPAM FILTERING

Mark Oliphant College uses department for education supplied Office 365 accounts, these come with a @schools.sa.edu.au email address; a separate @moc.sa.edu.au email address may be provided to as needed by the college.

Emails can be accessed anywhere with an internet connection; this can be done by configuring a personal device or accessing https://outlook.office.com/

The Department for Education provides a spam e-mail filter service to Mark Oliphant College for all users. However, in some instances spam email can reach our users. Users are provided with tools to flag/report spam in their mailboxes and are requested to report spam to ICT support via email to ict@moc.sa.edu.au A user is not to use the college or department for education email systems for spreading/sending/distributing spam e-mail.

If a user chooses to link a personal device to the Mark Oliphant College email system the user will be prompted to accept a set of security criteria, these criteria require a pincode/passcode on the device.

THIRD PARTY PARTNERS

Mark Oliphant College and its partners may utilise products that utilise third parties and services not otherwise mentioned explicitly within this agreement. Before using a product that uses third parties, Mark Oliphant College will conduct a risk assessment and implement risk management strategies before proceeding with the products use. While risk cannot be removed, we will only use a vendor where we believe it Is safe to do so.

WHAT IS THIRD PARTY DATA?

Third party data is any data that is collected by a business or other entity that does not have any direct interaction to our staff or students.

Third party data is often collected, aggregated, and in some cases sold to companies, to help them build advertising and or strategies. The recorded information is often anonymised and cannot be traced back to the individual.

CLOUD SERVICES – O365

Mark Oliphant College will utilise the expanded email service offered to students with additional services and will be known as Office 365.

Office 365 is a customised package of Microsoft Office 365, tailored for the South Australian public education system, and is offered at no additional charge to parents/guardians whilst their student remains enrolled at Mark Oliphant College.

Users at Mark Oliphant College will be able to download licenced versions of common Microsoft applications used in teaching and learning at no charge, for use on their device regardless of an internet connection. They will also have their own online storage space for files that can be shared with other students and teachers.

Below is some important information regarding the Office 365.

WHAT IS OFFICE 365?

Office 365 provides students with 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 their educational program.

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

- **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 a student (including 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 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 students can store, sync, update, and share files from any internet connected web-browser, and collaborate on Office documents.

  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 Office 365 users, including staff and students of other schools and preschools, but not anyone external to the Department for Education schools/preschools.

USING OFFICE 365 SERVICES

A number of services provided by Office 365 require internet access. When students are onsite internet access will be filtered by the College however access from home/off-site is not filtered by the College 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 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.

Users of Office 365 are responsible for the information/data in their Office 365 account and any important information should be backed up. 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 TO USE THE OFFICE 365 SERVICES?

The school / preschool requires written notification by 4pm Friday of the second week of term if you do not consent to your child using the additional Office 365 Services. Please use info@moc.sa.edu.au to notify the school.

HOW WILL MY CHILD ACCESS THE OFFICE 365 SERVICES?

Office 365 services can be accessed by students by logging into the department for education edpass student portal https://portal.edpass.sa.edu.au/.

ADDITIONAL READING

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

- Appendix A: DECD Student privacy and information summary
- Australian Government eSafety Commissioner https://www.esafety.gov.au/parents

CLOUD SERVICES – GSUITE

Mark Oliphant College will utilise the Google G-Suite for education and offer some of its services to students, these services will be known as G-Suite (formerly Google Apps).

G-Suite is a customised package of Google products, tailored for the South Australian public education system, and is offered at no additional charge to parents/guardians whilst their student remains enrolled at Mark Oliphant College.

Students at Mark Oliphant College will be able to use Google alternatives to Microsoft applications used in teaching and learning at no cost, some classes will use these products at the core of their classroom. Some programs may be used without an internet connection. They will also have their own online storage space for files that can be shared with other students and teachers within the school and moderators where required.

To provide and encourage a safe learning environment Mark Oliphant College has turned off access to the email (Gmail), chat (hangouts), and social (G+) components of G-Suite. Students will use their school provided email account in place of these services. Mark Oliphant College will continue to monitor and enable or disable G-Suite services that become available in the future in line with maintaining a safe learning environment for our students.

WHAT IS G-SUITE?

G-Suite provides students with a collaboration platform to create and/or upload/share content. This may include websites, presentations, written, audio, images and video material as part of their educational program.

All data and information within G-Suite is securely stored in geographically distributed data centres as a 'cloud' and provides the following services to students.

- **Docs / Sheets / Slides**
  Available anywhere any time on any device students will be able to access their work to submit, change or review. Collaboration features will enable real time commenting and editing with peers on the same document.

  Similar to Office Online and Microsoft products such as Word, Excel, and PowerPoint. These applications provide students flexible and friendly alternatives that integrate with the G-Suite experience

  With revision history and automatic saving, work entries can be easily followed, reversed, or restored. Work is saved continuously as editing occurs to allow students to continue on where they left off on another device; the right tool for the right job at the right time.

  Docs/Sheets/Slides can operate in offline mode for creating new files or files that have been flagged for offline use. There is no limit to the number of devices or locations that can be used to access content.

- **Classroom / Forms / Sites**
  With Google Classroom and Google Forms, classes can be created to distribute assignments, give quizzes, send feedback, produce a survey and see everything in the one place. Sites provides a simple way to produce websites that can be shown to peers without leaving the safety of the school community.

- **Drive**
  Google Drive is a cloud service where students can store, sync, update, and share files from any internet connected web-browser, and collaborate on Google documents. It can be used like a virtual storage device to transfer files and folders between computers including backups.

  Each student will receive unlimited storage space in G-Suite's cloud. By default all data and files are private, however they can be shared with other Mark Oliphant College approved G-Suite users, including staff and students of other schools and preschools, but not anyone external to the Department for Education schools/preschools.

USING G-SUITE SERVICES

A number of services provided by G-Suite require internet access. When students are onsite internet access will be filtered by the College however access from home/off-site is not filtered by the College 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 G-Suite services.

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.

Users of G-Suite are responsible for the information/data in their Office 365 account and any important information should be backed up. G-Suite 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.

G-SUITE OFFLINE ACCESS

G-Suite applications can be installed on a computer or mobile device (personal device) for offline use.

Although unlikely, it is possible that installing G-Suite 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 Docs, Sheets, Slides or Drive application(s).

To install G-Suite in offline mode follow the google support article; https://support.google.com/docs/answer/6388102

WHAT IF I DO NOT WANT MY CHILD TO USE THE G-SUITE SERVICES?

The school / preschool requires written notification by 4pm Friday of the second week of term if you do not consent to your child using the G-Suite Services. Please use info@moc.sa.edu.au to notify the school.

HOW WILL MY CHILD ACCESS THE G-SUITE SERVICES?

G-Suite services can be accessed by students by logging into the Mark Oliphant College portal or by visiting any google service and signing in. e.g https://drive.google.com

ADDITIONAL READING

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

- Appendix A: DECD Student privacy and information summary
- Australian Government eSafety Commissioner
  https://www.esafety.gov.au/parents

RESPONSIBILITIES

Mark Oliphant College will

- Do its best to enhance learning through the safe use of ICT. 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 User Agreement s
- Respond to any breaches in an appropriate manner and as directed by school leadership and or principal
- Provide members of the school community with cyber-safety education designed to complement and support the User Agreement initiative.
- Store a current version of this document in accessible locations.
- Welcome enquiries at any time from parents/caregivers/legal guardians or students about cyber-safety issues.

For the Student: My responsibilities include…

- Reading this User Agreement carefully.
- Following the cyber-safety strategies and instructions whenever I use the school's ICT.
- 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 ICT equipment.
- Asking the home group teacher if I am not sure about anything to do with this agreement.

CONSEQUENCES

- Where there is a contravention of this policy, consequences will include any or all of the following dependant on severity.
    - Re-imaging the laptop which may result in the loss of data if back-ups have not been kept up to date.
    - Locking or disabling of the device from college infrastructure
    - Remote deletion of files and or folders (e.g. Copyright materials and/or unapproved software)
    - Disablement/suspension of ICT user account
- Other sanctions may be imposed as appropriate and determined in consultation with ICT Management and the Principal.

BRINGING YOUR OWN PERSONAL DEVICE

OVERVIEW

Whilst continuing the Mark Oliphant College Laptop Program, the school is looking to expand the students' options for learning through a BYOD device initiative. As some students already possess a suitable device at home, Mark Oliphant College want their students to be able to not only save families money through either the laptop program or BYOD, but also reduce our carbon footprint by reducing the need for multiple devices. Whilst a student uses a BYOD device, they will need to comply with the policies set by the school and the Department for Educations Cyber Security guidelines and device compliance.

MINIMUM TO RECOMMENDED SPECIFICATIONS

The College BYOD device initiative supports Windows and Chromebook devices as they are compatible with the Department and College ICT systems and software.

Operating System	Storage	Memory (RAM)	Screen Size
Windows 11	*256GB – 512GB*	*8GB – 16GB*	*13" – 14"*
Chromebooks	*32GB – 64GB*	*4GB – 8GB*	*11" – 13"*

NB: Recommended devices for CAD, Media Arts & Students needing windows applications are Windows 11 devices. Parents can contact the school to query whether their existing devices are suitable.

BYOD SERVICES

Approved Students can connect their personal laptops to the Mark Oliphant Wireless Network (*MOC – BYOD)*. Student devices will not be permitted onto the wireless network without a signed and approved BYOD Device Compliancy Form. Any students using non approved devices may lose their laptop for the day with immediate contact to caregivers.

The BYOD initiative will allow students to:

- *Access the school's wireless network.*
- *Limited technical support.*
- *Access to the internet.*
- *Access to Printing (Papercut).*
- *Access to the schools' web services and portal.*

ACCESS THE SCHOOL'S WIRELESS NETWORK

Student will have the ability to connect to Mark Oliphant College's ***MOC – BYOD*** Network. Bringing your own device will not allow the use of ***MOC – Curric*** Network. BYOD Devices found to be connecting to ***MOC – Curric*** will be in violation of *ICT Cyber Security Standard.*

- *Users are required to authenticate on the* **MOC – BYOD** network *to ensure that any internet or network logs can be traced to a specific user and is isolated from school-based devices and servers.*
- *The use of the* ***MOC – Curric*** network is prohibited.
- *Hotspot is not allowed to be used whilst on schools' grounds.*

TECHNICAL SUPPORT

Students who require support for connecting their account to the network can obtain assistance from ICT Services, however any technical or software faults should be returned to the place of purchase or a preferred repairer. If the user has a repair warranty on their device, it's advised the individual goes through the warranty before use of a 3rd party repairer.

INAPPROPRIATE USE

Students are expected to follow the *ICT User Agreement* and all rules specified in the handout all users sign before being allowed to connect to the network. (ICT User Agreement 2023). An overview of inappropriate use of a BYOD is specified but is not limited to:

- *Using your device on a hotspot while on campus*
- *Using your device to access inappropriate material through Hotspots, VPN (Virtual Private Network), embedded websites or other forms of policy avoidance while onsite.*
- *Distributing inappropriate material locally stored on your personal device.*
- *Distributing programs or information illegally, e.g., stolen or modified programs for free use.*
- *Attempting to use sites with content that is violent, racist, sexist, pornographic, dominated by offensive language and/or illegal in any way.*
- *engaging in cyber bulling or e-crime*
- *taking photographs of individuals and place these images on the internet or in a public forum without their expressed permission.*
- *Sharing school data or students' information without consent.*

By connecting a personal device to the network, the user's device becomes subject to the controls and requirements defined in this standard, including the department's authority to remotely wipe the device should a security compromise be suspected.

Conditions of use Extending this standard's requirements, department-owned and personally owned mobile phones and tablets used to connect with the department's ICT assets require acceptance and implementation of the following conditions:

- *The user of the device must accept the installation of a department-controlled profile, where it is deemed necessary by ICT Services or the site leader, on the device. This profile must enforce certain configuration parameters, which may include, where possible:*
- *An inactivity timer lock with a passcode*
- *A maximum of 60 days of mail and calendar items stored on the device o multi-factor authentication for access email accounts on initial set up and each time the user account password is changed.*
- *Encryption.*
- *The user of the device is responsible for ensuring that device software is updated appropriately to ensure security risks are not introduced to the department's infrastructure when connected.*
- *The department will reserve the right to erase the contents of the device and/or disable the device at any time, at the discretion of ICT Cyber Security or site ICT personnel. This includes personal devices that hold departmental data if staff choose to user personal devices for this purpose. Site leaders (for schools) or ICT Services for corporate staff must obtain and refresh acceptance of these requirements from staff prior to issuing a mobile device or allowing a personal device to connect to the network. A template user agreement is available from ICT Services.*

Site leaders (for schools) or ICT Services for corporate staff must obtain and refresh acceptance of these requirements from staff prior to issuing a mobile device or allowing a personal device to connect to the network. A template user agreement is available from ICT Services.

https://edi.sa.edu.au/__data/assets/pdf_file/0009/606978/ict-cyber-security-standard.pdf

(ICT Cyber Security - Department for Education South Australia, 2023)

Mark Oliphant College
ICT User Agreement

STUDENT DETAILS

GIVEN NAME: ..... SURNAME: .....
(Please Print) (Please Print)

1. We have read and understood this device and ICT User Agreement, incorporating Cyber-safety and we are aware of the College's initiatives to maintain the care, use and management of devices in a cyber-safe learning environment. We understand that failure to comply with the User Agreement could result in recall of the device and/or costs associated with repairs or replacement of the device while in the care and of the student.

My responsibilities as a Parent/Caregiver include:

- Reading this User Agreement carefully and discussing it with my child so we both have a clear understanding of our roles in using technology devices in learning
- Ensuring this User Agreement is signed by my child and by me and returned to the College
- Encouraging my child to follow the cyber-safe strategies
- Contact the College if there is any aspect of this User Agreement I would like to discuss.
- Contact the College if I wish to opt-out of mentioned cloud services

This agreement will remain in force as long as your child is enrolled at Mark Oliphant College

I have read the ICT User Agreement. I understand my responsibilities regarding the use of equipment and the Internet. In signing below, I acknowledge that I understand and agree to the responsibilities, conditions, and liabilities of the ICT User Agreement. I understand that failure to comply with the ICT User Agreement could result in the recall of any supplied equipment and user accounts.

PLEASE RETURN THIS SECTION TO THE COLLEGE AND KEEP A COPY OF THE AGREEMENT FOR FUTURE REFERENCE.

....
Student Signature Date

. ...
Parent/Guardian 1 Signature Date

. ...
Parent/Guardian 2 Signature Date

APPENDIX A: STUDENT PRIVACY INFORMATION SUMMARY

WHERE WILL THE INFORMATION/DATA BE LOCATED?

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.

G-Suite offers the similar Cloud based services as Office 365 however the servers are operated under United States law. The location of data for G-Suite is within Googles network of geographically distributed data centres. More information can be found here:
https://www.google.com/about/datacenters/inside/locations/index.html

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 Office 365 and G-Suite services will be stored in the data centres. This may include text, images, photographs, sound and multimedia (e.g. videos).

Microsoft and Google does not access, use, track or collect information or data about the student, other than to deliver the Office 365/G-Suite service on behalf of the Department for Education. 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 Office 365 and/or G-Suite service. They can share their information and data with other Office 365 or G-Suite users of the same platform; this includes staff and students from other the Department for Education schools or preschools. Anyone external to the Department for Education is unable to access student information and data.

Processes are in place to allow authorised Department for Education 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 the Department for Education or if required to do so by law. Google will only disclose information and data with direct requests from government and actively pursues limiting the amount of supplied information to only that which is required

HOW SAFE IS THE STUDENT'S INFORMATION AND DATA?

Microsoft's Office 365 Service (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 the Department for Education. Additionally Microsoft's Office 365 Service is certified to several international security standards.

Googles G-Suite for education has a strong security and privacy focus with respect of these two elements being a core priority of Google. More information can be found at the following websites.

Google Cloud Trust: https://support.google.com/googlecloud/trust/?hl=en
GSuite Security: https://gsuite.google.com/security/