

Contents

| | |
|--|---------|
| Why 1 to 1? | Page 2 |
| Selecting a device | Page 2 |
| Year 7-9 iPad Program Overview | Page 2 |
| Year 10-12 BYOTech Program Overview | Page 2 |
| Purchase Options | Page 3 |
| Warranty | Page 3 |
| Finance Options | Page 3 |
| Insurance | Page 4 |
| Expected Use | Page 4 |
| Everyday Use Tips | Page 5 |
| Year 7-9 iPad Program Full Details | Page 7 |
| Getting Connected | Page 7 |
| Setting up the iPad | Page 7 |
| Configuring the Device for Melba | Page 8 |
| Backing up | Page 9 |
| Creating an Apple ID | Page 10 |
| Redeeming an iTunes card | Page 11 |
| Family Sharing | Page 11 |
| Year 10-12 BYOTech Program Full Details | Page 12 |
| Approved Devices | Page 12 |
| Antivirus | Page 13 |
| Storage | Page 13 |
| Required Software | Page 14 |
| Free Software | Page 15 |
| Technical Support | Page 15 |
| Theft and Damage | Page 15 |
| Security | Page 15 |
| Acceptable Use | Page 16 |
| Staying Safe Online | Page 17 |
| Unwanted Contact | Page 17 |
| Cyberbullying | Page 17 |
| Online Friends | Page 18 |
| Helpful Resources for Parents | Page 19 |
| Dealing with Overuse | Page 20 |
| Free Home Internet Filtering | Page 22 |
| What to do if things go wrong | Page 23 |
| Frequently Asked Questions | Page 24 |

Why 1 to 1?

We live in an ever changing world, and the pace of that change is increasing. The era when schools and teachers were the sole source of knowledge is gone. This is a time in which Cynthia Sin Nga Lam, age 17, from Melbourne can invent a solar powered water purification system that might change the lives of millions. Or Daniela Lee, age 17, and Sadhika Malladi, age 16, of San Jose California, can create a new test for breast cancer. From ideas that can help one individual learner to ideas that can change the world, access to ICT (or Information and Communication Technology) is reinventing how people learn and grow.

Selecting a device

At Melba, we are clear about the purpose of our 1 to 1 devices – they are, first and foremost, tools for learning. To this end, they must be dependable, flexible and affordable. At the junior levels, despite a competitive market, the iPad is still the clear winner in this regard. At senior levels, students are more flexible in their needs and more able to manage a device properly; within limits, they may use the device of their choice (Phones are **not** acceptable)

Years 7 - 9 iPad Program Overview

Any iPad from iPad2 onward is acceptable at these levels. The iPad Mini is not recommended to be carried through to senior level; its screen is just too small. An important consideration with the iPad is the level of memory the device has. Memory options start at a base of 32 Gigabytes all the way up to 256 Gigabytes. The greater the memory, the more information the iPad can store; the memory in the iPad is not upgradable. A 32Gb model is fine for most situations.

Please note: The College does not allow 3G or 4G enabled iPads to be used in the school.

This is because we cannot control the internet content on a 3G/4G device. If an externally sourced iPad is brought to the College that is capable of its own internet connection, the SIM card **must** be removed at all times while at school.

Please note also that the iPad is the only approved device at Junior School.

Years 10-12 BYOTech Program Overview

At Years 10-12, there are a range of devices available to students to be connected to the Melba network and used in class. The range of acceptable devices and the conditions that accompany their use are detailed in the [Senior BYOTech section](#).

Students must nominate and connect **only one approved device**. This device must be registered with Melba's mobile device management system and must remain registered at all times. No other device will be permitted to be connected for that student.

Purchase Options

Melba College has a partnering agreement with JB HiFi to provide digital devices to students at competitive prices. There is no financial benefit to the College; this is a service to families. Purchases of digital devices and insurance are available via a portal on the Melba College website

Links to the portal can be accessed from the Melba College website at <http://melba.vic.edu.au/learning/digital-learning>

Digital devices purchased via the purchase portal may be financed through FlexiRent to help spread the costs over a longer time frame. Additionally, insurance for the device may be arranged at the time of purchase; **this is highly recommended for new devices**.

Alternatively, families may wish to purchase their child's device from a supplier of their choice. This is a perfectly acceptable alternative. Many families with children in 7-9 will already have an iPad at home. These are welcome to be used at Melba College provided it is an iPad 2 or better and is in full working order with no damage.

Many families of 10-12 students may have a device such as a laptop at home that their child would like to use at school. This is fine provided the device meets the requirements detailed in the [Senior BYOTech section](#) of this guide.

Warranty

For iPads, the standard Apple warranty terms and conditions apply. Tech support staff will be able to assist in determining whether an issue is one related to warranty or something else. In the case of a warranty claim staff will direct you to the nearest Apple centre.

For other devices, manufacturer warranty applies; however, JB Education is the factory service agent for all non-Apple devices offered on the purchase portal and so can handle claims directly. Extended and enhanced warranties with on site priority support can also be purchased for these devices via the purchase portal.

Finance Options

Leasing is a solution for education equipment, and keeps your family up with the latest technology without impacting on cash-flow or burdening families with big upfront costs. The FlexiRent finance solution allows you to manage monthly lease

payments, rather than having to manage a big upfront cost. With FlexiRent, families have the peace of mind of knowing that their equipment is covered for accidental loss or damage .

Families can choose a 12, 24 or 36 month term with a fixed monthly payment that best suits their students' requirements. At the end of their leasing term, students can return the equipment, swap it, offer to buy it, or continue to lease the equipment on a 'month to month' agreement. The choice is up to the family. For further information, please refer to <https://www.flexirent.com.au>

Insurance

For devices purchased via the purchase portal, JB Hi-Fi Education Division can provide damage and theft insurance at competitive rates.

JB Hi-Fi manage the entire claims process to avoid any delays in devices being repaired, ensuring the device is serviced and returned in a timely manner.

Expected Use

To protect the safety of your child and the wider community of the College there are some strict conditions attached to the right to use an Digital Device at Melba. These are as follows:

When using an Digital Device, students attending Melba College must:

- ★ Be a safe user whenever and wherever they use technology
- ★ Use the Device for learning purposes as directed by the teacher
- ★ Be responsible whenever and wherever they use technology, and support others by being respectful in how they talk to, work with, or socialise with them, and never participate in online bullying (this includes forwarding messages and supporting others who are engaging in harmful, inappropriate or hurtful online behaviour)
- ★ Report to an adult if they feel uncomfortable or unsafe online or see others participating in unsafe, inappropriate or hurtful online behaviour
- ★ Act responsibly and not use the device to find, create or send information that might be harmful, inappropriate or hurtful to them or anyone else

When at school they will agree to at all times to:

- ★ Behave according to the school's Code of Conduct
- ★ Protect their own privacy and that of other students by not giving out personal details ([See Staying Safe Online section.](#))
- ★ Use appropriate language when talking to and working with others online and never participate in hate mail or acts of harassment

- ★ Use the Internet at school for educational purposes and use the equipment properly
- ★ Use social networking sites for educational purposes and only as directed by teachers
- ★ Not deliberately enter or remain in any site that has obscene language or offensive content (e.g. racist material or violent images)
- ★ Abide by copyright procedures when using content on websites (ask permission to use images, text, audio and video and cite references where necessary)
- ★ Think about how they use content posted on the Internet and not simply copy and paste information from websites
- ★ Not interfere with network security, the data of another user, or attempt to log into the network with a user name or password of another student
- ★ Not reveal their passcode to anyone except the system administrator or teachers

Talk to their teacher or another adult if:

- ★ They need help online
- ★ They feel that the welfare of other students at the school is being threatened
- ★ They come across sites which are not suitable for our school
- ★ Someone writes something they don't like, or makes themselves or their friends feel uncomfortable, or asks them to provide information that they know is private.

When using a Digital Device as a camera they will.....

- ★ Only take photos and record sound or video when it is part of a class or lesson
- ★ Seek permission from individuals involved before taking photos, recording sound or videoing them (including teachers)
- ★ Seek written permission from individuals involved before publishing or sending photos, recorded sound or video to anyone else or to any online space
- ★ Seek teacher permission before uploading any content to websites (e.g. blogs)

Everyday Use Tips

- ★ **Not every class** will involve the use of technology. Students will spend as much, if not more, time using pen and paper and writing.
- ★ **The teacher will make the decisions** on when Digital Devices may be used, *not the student*. There will be times at which teachers may require students to pack away their device for the lesson.
- ★ **Playing of games** on Digital Devices is discouraged, other than those a teacher directs students to.

- ★ **Playing any game** which is other than PG-13 rated is not allowed.
- ★ **The college provides many ways to communicate electronically:** use of any other means such as Snapchat, Kik or anything similar during class is strictly forbidden.
- ★ **Only the students' school email account** should be used during school hours
- ★ **Any communication** to teachers must only use the students' school email account or Compass.
- ★ **Any information** passed across the college network connection is NOT private. While staff do not constantly monitor every student action, all communications and browsing histories are logged and recorded to each user. Students should be aware of this.
- ★ **Cyberbullying** in any form is subject to a zero tolerance policy.
- ★ **A Digital Device not in a cover** generally doesn't survive very long and is expensive to repair. A cover should be used at all times on any tablet type device.
- ★ **Every school day** the Digital Device must come to school fully charged with storage space available and must be fully functional—this is the responsibility of every student, every day.
- ★ **Excuses that an Digital Device has a technical issue** when no attempt has been made to get technical support at school will not be accepted and sanctions will apply. The good working order of the Digital Device is the student's responsibility alone.
- ★ **Non connected Digital Devices** are not permitted to be used in class.
- ★ **Digital Device use outside of class time** is not encouraged and they should only be used in designated areas.
- ★ **In the case of Junior iPads, the Mail app** must be set up and connected to the student's Melba College Google account at all times. Students will be guided through this in the first week of Year 7 classes.
- ★ **Students are expected to link** their Digital Device Calendar app to the Melba calendar and use the Digital Device as a planner to record their school activities, deadlines and commitments. Students will be guided through this in the first week of Year 7 classes.
- ★ **Digital Devices must be kept in a locked locker** when not carried by students. Digital Devices should not be left at school overnight but instead can be left with the ICT Support Centre for safekeeping.
- ★ **Students should read the rules on Digital Device camera usage carefully** and be aware that unauthorised photography is considered to be an extremely serious infringement of other people's privacy and will be met with severe sanctions.

Year 7-9 Junior iPad Program

Getting Connected

The iPad needs a wireless network before it can connect to the Internet. Fortunately, iPads are very clever at configuring themselves for most networks, and provided you have the correct security credentials are very easy to connect. Melba College, however, has a high security network that requires the installation of a profile and encrypted certificates to each device connected. Prior to the commencement of the school term you will receive, to the email address you have nominated to the school, a web address and a code. Navigating to this address on the iPad and inputting the code supplied will configure the device for the Melba network and trigger the downloading of any free apps specified by the College. This way the iPad will be ready to go day one!

Setting Up the iPad

All setting up of the device, including configuring the device for the Melba network, can be done by students and parents. There are some very good reasons for this; the device can be set up and used over the Christmas break by students, and it helps students and parents become familiar with the device.

You will need to make an Apple ID. This is a fairly simple procedure and a good guide is included in this booklet at the bottom of this section in *Configuring the Device*.

Even if you have an **Apple ID** we suggest you create another specifically for this device and your child and use family sharing. This way you do not need to give your Apple ID credentials to your child. This is particularly pertinent if you have connected a credit card to your original account; you can create a new account for this device that has no credit card attached to it and just operates from iTunes vouchers. Instructions for how to do this follow in this booklet. iTunes vouchers can be bought at supermarkets, convenience stores and variety chains and are sometimes even discounted for short periods.

Once you have an Apple ID, you'll need to download the required apps. The free required apps should be delivered to your iPad automatically when you configure it for the Melba wireless network, although this is not always 100% reliable. You'll need to check the list of required apps on the College website at <http://melba.vic.edu.au/learning/digital-learning/> and manually download any missing

apps. Any paid apps will also need to be manually installed.

If you use the iPad to browse the Melba site, you'll find each app has a link that when clicked will take you directly to the app store and the app in question. To download an app, just click the price (e.g. \$19.99) or the word **Free** if it is a free app. The app store will prompt you for a voucher code if you have not already applied one to the account.

The app will download and install automatically.

The apps will be divided into Tier 1 and Tier 2, and Year level. Tier 1 apps are mandatory and **MUST** be installed on the device. Tier 2 apps can be installed when needed but the iPad **MUST** have free storage space left over for them to be installed if required.

Most apps specified are free. However, there may be some with a small cost attached from year to year. If you supply your own device you must still comply with this requirement. All iPads will be audited in Term 1 to ensure they do, in fact, have all the required apps installed.

Please make sure the device has a passcode and that this is recorded somewhere safe.

Configuring the Device for Melba

Step 1

Please go to *Settings > About* and change the name of your iPad to the student code that was included in the connection email sent to the email address you registered with the school.

If you do not complete this step, your iPad will not remain connected to the Melba network. The iPad must remain named by student code for the duration of its connection to Melba College.

Students attempting to enrol iPads with inappropriate device names will be subject to serious sanctions, and will be unable to remain connected.

Step 2

You will need to be connected to a network with internet access for this next step. This could be your home network, a public WiFi hotspot, or even a hotspot from your phone.

A link and a connection code will have been emailed to the account you registered with the college as your preferred email contact address. Simply click the link and input the connection code when the page loads.

You will be asked to accept a certificate and a profile, and to trust both. Please do so with both. Within a few minutes, your iPad will register itself with our Meraki Mobile Device Manager and will be configured remotely for the Melba network.

Step 3

Shortly after Step 2, you will be prompted by the app store for your iTunes password. This is so Meraki can download the connection management app. Once downloaded and installed, the app will prompt you to select whether you want Meraki to have access to location services. The sole function of this is to determine the position of the iPad if it is lost or stolen. You may choose to turn this function on or off, bearing in mind tech staff will not be able to locate your iPad if it goes missing and location services are turned off. Any free Tier 1 apps specified by Melba College will now automatically download; to make this process more straightforward, make sure you have the App Store set to only ask for a password on the installation of paid apps (i.e. not for free apps).

The Meraki app must remain installed as it allows tech staff to manage the connection at Melba College. iPads that do not have the app present will be quarantined from wireless connection and a reconnection fee may be levied to restore the device's access to the Melba network.

The device is now fully functional for connecting at school

Backing up

This is very important for iPads used in education. The information contained on the iPad may be vital for success in a subject, for example an essay or a project. Once the iPad is configured for Melba College, important files can be backed to the college network and/or to the college Google Apps Suite.

Apple's own iCloud, though, should be a first line of defence against data loss.

Please make sure that iCloud backup is turned on from day one of school at Melba College. In the case of an iPad being damaged, Apple frequently elects to replace a device rather than repair it, and they will NOT transfer the data for you. The user must do this via an iCloud backup prior to a repair.

How to backup with iCloud.

- ★ Make sure you are connected to a wireless network with an internet connection

- ★ Go to *Settings* > [your iTunes Account Name], and tap *iCloud*. If you're using iOS 10.2 or earlier, go to *Settings*, then scroll down and tap *iCloud*.
- ★ Tap *iCloud Backup*. If you're using iOS 10.2 or earlier, tap *Backup*. Make sure that iCloud Backup is turned on.
- ★ Tap *Backup Now*. Stay connected to your Wifi network until the process completes.
- ★ You can check the progress and confirm that the backup has completed. Go to *Settings* > [your iTunes Account Name] > *iCloud* > *iCloud Backup*. Under *Back Up Now*, you'll see the date and time of your last backup.

How to backup with iTunes

- ★ Open iTunes and connect your device to your computer.
- ★ If a message asks for your device passcode or to Trust This Computer, follow the onscreen steps.
- ★ Select your iPad when it appears in iTunes.
- ★ If you want to save Health and Activity data from your iOS device, you need to encrypt your backup: Select the box called *Encrypt [device] backup* and create a memorable password. If you don't need to save your Health and Activity data, you can make a backup that isn't encrypted - just click *Backup Now*
- ★ When the process ends, you can see if the backup finished successfully on the Summary screen in iTunes. Just look under *Latest Backup* to find the date and time.

To restore a device after reset

- ★ Turn on your device
- ★ You should see a Hello screen
- ★ Follow the steps in the iOS Setup Assistant until you get to the Setup screen
- ★ Select *Restore* from iCloud Backup
- ★ Select a backup.

Create your Apple ID

- ★ Open the App Store or iTunes Store on your iOS device.
- ★ Choose any free app, song, video, or book. Tap *Free* next to the item, then tap again to get it. When you're asked to sign in with an Apple ID, tap *Create New Apple ID*.
- ★ Follow the onscreen instructions.

★ **When you're asked for payment information, choose None.**

After you enter all of the information required, you'll be asked to verify your Apple ID by email. You must verify your Apple ID before you can begin using it.

This is the safest way to create an Apple ID. This way, unless an iTunes voucher is applied to the account there is no balance available to download material with a cost. If you wish, you may add a credit card or bank account as a payment method at anytime either via iTunes on a computer or the Apps Store on the iPad.

Redeeming an iTunes Card



Turn over your iTunes card and peel off the label to reveal the 16 Digit hidden code

- ★ On your iPad, tap *App Store*.
- ★ Tap *Today*, and then tap your Apple ID icon.
- ★ Tap *Redeem*.
- ★ Sign in with your Apple ID.
- ★ Tap *Use Camera*. Make sure to follow the onscreen instructions to capture the redemption code. Choose *Use Credit for iTunes or App Store*.
- ★ Tap *Done*.

Family Sharing and Apple IDs for kids

From IOS 8 onward, Apple have introduced Family Sharing. Apps are automatically shared between family members . Apple ID for Kids means that parents can create Apple IDs for students under 13 that are linked and under the supervision of the parent account.

(Please note - If you're the organiser for a Family Sharing group and want to share purchases with your family, you're required to have a payment method on file. A payment method is also required to set up accounts for children)

There are some great new features on the latest iOS 12.1 if you have family sharing. When it's enabled you'll be able to place restrictions on what can be done on the iPad using [Parental Controls](https://support.apple.com/en-au/HT201304) (<https://support.apple.com/en-au/HT201304>) and you'll even

be able to monitor and set rules for screen time e.g. screens off after 9pm or no gaming after 9.00am or even 2 hours of gaming per week using the [Screen Time](https://support.apple.com/en-au/HT208982) function (<https://support.apple.com/en-au/HT208982>)

Full instructions here -

Family Sharing <https://support.apple.com/en-us/HT201088>

Apple IDs for Kids <https://support.apple.com/en-au/HT201084>

Years 10 - 12 Senior BYOTech Program

Please note that it is mandatory for senior students to have access to a device which complies with the device requirements, is connected to the Melba network and is available for every class, every day.

All devices will be connected through EduSTAR; this facility will also manage student identities and access. Additionally, all connected devices must have Meraki mobile device management software installed at all times. The College will supply this software and monitor its functionality on each device. Removal of the software will result in immediate disconnection.

Students must nominate and connect **only one approved device, total**. This device must be registered with Meraki and remain so at all times; no other device will be permitted to be connected for that student. An attempt to breach this policy may result in permanent disconnection.

Approved Devices

Students may use either a tablet (with IOS or Android) or a laptop (with Windows or Apple OS X) - **PHONES ARE NOT APPROVED FOR CONNECTION**

Laptops

Windows

The laptop must have Windows 7 or later installed.

It must have an approved Anti-Virus installed, up to date, and running at all times.

Mac/OS X

The laptop must have Apple OS X 10.7 or later installed.

It must have an approved Anti-Virus installed, up to date, and running at all times

Tablets

Apple/iOS

Any iPad, including the Mini, that has IOS 9 installed.

Generic Tablet (least recommended option)

Any tablet with a 7 Inch display or larger that has Android 7 Nougat or later installed.

Approved Anti-Virus

Essentially any reputable and commercially available antivirus software that is up to date and supports real time virus scanning is suitable. The antivirus software listed below are specifically approved. *Note that students may access the College's enterprise grade Microsoft System Centre Endpoint Protection (SCEP) at no cost- see technicians for details.*

(Not required for IOS or Android)

- AVG
- Norton Securities / Semantic
- Malwarebytes (Paid version only)
- Kaspersky
- McAfee
- Avast
- Trend Micro
- Microsoft Security Essentials
- Windows Defender

Required Software

Melba College uses a mobile device management platform called Meraki, which assists in maintaining and monitoring the connection of any device on the network. Meraki continues to operate when the device is not connected to the Melba network and performs a degree of monitoring whenever the device is connected to the internet.

For both IOS and Android devices, Meraki can report what apps are installed, the last known location of the device, and the current connection state. Location information is only available if the user has opted to turn on the location services for Meraki. This is a useful feature if the device is lost or stolen; however, this information is only able to be accessed by the ICT Manager at Melba and the two senior technicians. The user may opt to have it on or off. Meraki also allows a capacity to remotely lock and unlock the device, clear the passcode, and selectively or fully wipe the device; again, useful in an instance of the theft or loss.

For Windows and OS X devices, the Meraki MDM client software has greater capabilities which both parents and users need to be aware of. It must be stressed that only our Melba senior ICT staff will have access to any of these capabilities and that they will never be used without the knowledge and consent of users; they exist only to provide remote assistance and security in the case of a lost or stolen device.

The Meraki client allows an administrator to (on Windows and OS X):

- Initiate a remote desktop session
- Run a terminal command (i.e. operate Command Prompt)
- Remotely install software
- Securely erase the device
- Lock the device
- View connection state and the IP of a current connection.
- View the name of the connected network

What the Meraki Client cannot do

Record or view a user's actions

Record or view browsing history outside school

View or record any information from the screen without user permission

Access any files or folders on the device

Monitor the keyboard

Run any installed software without user permission.

Activate any facility on the device without the user's permission.

Free Software

Office 365

Early in 2019 Melba College will be offering students signed in to the BYOT program access to Microsoft Access 365 at no cost.

The EDUstar Catalogue

Students will also have access to the EDUstar catalogue of subsidised commercial software at no cost to install on their device.

Technical Support

Technical support staff will endeavour to assist students with simple technical problems but will be unable to provide in-depth or complex technical support. The student ICT support team, called TECHNIC, is in place and will be able to provide greater support by arrangement. It is expected that students will largely support and manage the devices themselves. A troubleshooting self help knowledgebase will be accessible to students via the Helpdesk at <http://help.melba.vic.edu.au/>

Insurance/Theft/Damage

The College will not insure or indemnify any device from theft or damage. The student must take full responsibility for the device at all times. It is strongly suggested that device remains in a **locked** locker at break times at school.

Security

Any device connected must be secured by means of a passcode, fingerprint scanner or username and password irrespective of the type of device. *If for any reason the device cannot have a locking function applied, it cannot be connected to the Melba network.*

The device must be locked at all times when not in use.

No “[jailbroken](#)” or “[rooted](#)” devices may be connected

Acceptable use

Please see the section regarding expected use earlier in this booklet. For a copy of the full acceptable use policy at Melba College see here -

<http://melba.vic.edu.au/learning/digital-learning/ict-use-agreement/>

Staying Safe Online

A Cyber Safety guide for parents and students

Unwanted contact

Sometimes you can meet someone or see something online that is offensive, upsetting or makes you feel uncomfortable. This could be communication from an online friend who starts asking personal questions or sends you photos or material that you either don't like, find unpleasant or find confronting. In some cases, it may be from someone you know in person, but what they've sent seems offensive or obscene. What should you do?

Tell someone. Tell a trusted adult like your mum, dad or a brother or sister who can help.

Don't respond to messages- leave the site or chat session immediately.

Block the contact using your 'ignore' list or with filtering software.

Keep the evidence. This can be useful in tracking the person posting unsuitable material.

Report it. Contact your ISP and/or phone provider, or the website administrator, as there are actions they can take to help. Your parents can help with this if needed. You can also report it to the police if there is a threat to your safety.

Set your profile to 'private' so your personal details are kept private and it's harder for people you don't know to contact you.

Don't open messages from people you don't know. They could contain viruses or be trying to sell you something.

Remember, if you want to talk about a problem with unwanted contact, call Kids Helpline on 1800 55 1800, visit their website, or contact the Cybersmart Online Helpline service.

Cyberbullying

The same rules apply online as in real life about how to treat other people. Unfortunately, people don't always treat each other well online, and you, or a friend, may find that you are the target of cyberbullying. You might be teased or have false rumours spread about you online, receive nasty messages or even threats. It can

happen in school, or out of it, any hour of the day, from people you know, and sometimes people you don't know. It can leave you feeling unsafe and alone. No-one has the right to bully another person. At its most serious, cyber bullying is illegal and can be investigated by the police.

Ignore it. Don't respond to the bully. If they don't get a response they may get bored and go away.

Block the person. This will stop you seeing messages or texts from a particular person.

Tell someone. Tell an adult you can trust. You may want to talk to your mum, dad or a brother or sister or any teacher. Or you can contact the Cybersmart Online Helpline service, call Kids Helpline on 1800 55 1800, visit their website.

Keep the evidence. This can be useful in tracking the bully down. Save texts, emails, online conversations or voicemails as evidence.

If it happens at school, speak immediately to a Student Manager, an Assistant Principal or any staff member.

Report it to;

- ★ **School**—any teacher at Melba can start the response to help you with a bullying or cyberbullying problem.
- ★ **Your ISP** and/or phone provider, or the website administrator— there are actions they can take to help.
- ★ **The police**—if there is a threat to your safety the police will help. Call Triple Zero (000) or Crime Stoppers on 1800 333 000.

Online friends

Chatting to friends using social networking sites can be a great way to keep up to date. Meeting new friends online is also fun. You can meet people online that are into the same bands or sports, or you can keep in touch with old friends who have moved away. But while there are lots of good points about keeping in touch, there are also some risks with meeting people online—especially if you don't know them in real life.

To help stay safe while you message, remember some simple tips:

Be careful who you trust online. A person can pretend to be someone they are not.

Choose your friends. While it's good to have a lot of friends, having hundreds of online friends makes it harder to control what happens to information you post online. Don't accept friend requests if you're not sure about the person.

Keep your friends list manageable by making sure that the majority of your friends

are your real life ones. It's a good idea to occasionally spring-clean your friends list to remove people you don't know in person, especially if you haven't heard from them in a while.

Keep your personal details private. Use an appropriate handle or username instead of your real name where there may be lots of people you don't know. Don't give anyone on the internet your name, address, phone number or any other personal details if you are unsure.

Set your profile to private and use the privacy settings to control who can see your photos and posts.

Always keep your password secret. Don't even share it with your friends

Help stop cyberbullying! Stand up and speak out.

It can be hard to know if your friends are being cyberbullied. They might keep it to themselves. If they are being cyberbullied, you might notice that they may not chat with you online as much, suddenly receive lots of SMS messages or are unhappy after they have been on the computer or checked their phone messages. They may stop hanging around with friends or have lost interest in school or social activities.

If you see or know about cyberbullying happening to a friend, support them and report the bullying. You'd want them to do the same for you. Don't forward on messages or pictures that may be offensive **or** upsetting to someone. Even though you may not have started it, you will be seen to be part of the cyberbullying cycle.

*Students should remember to treat others
as they would like to be treated when
communicating online*

Helpful Cybersafety resources for parents

Office of the eSafety Commissioner - <https://esafety.gov.au/education-resources/iparent>

Australian Government - <https://www.staysmartonline.gov.au/>

Australian Federal Police - <https://www.thinkuknow.org.au/>

Youth Central (Vic Gov)- <http://www.youthcentral.vic.gov.au/web-social-safety>

Cyber Safe Kids - <http://www.cybersafekids.com.au/>

Google - <https://www.google.com/safetycenter/families/start/>

Law and the Internet - <http://www.lawstuff.org.au/>

Telstra's Cyber Safety resources - <http://www.telstra.com.au/abouttelstra/advice/internet/>

Yahoo's Cyber Safety resources - <http://au.safely.yahoo.com/>

Facebook(official) - <https://www.facebook.com/safety/groups/parents/>

Facebook – a great downloadable resource for parents -

<http://www.connectsafely.org/pdfs/fbparents.pdf>

Tagged

A short movie every parent should watch with their teenage child

<http://www.cybersmart.gov.au/tagged/>

Dealing with overuse - help for parents

Everybody understands how a device is used at home

Public not private devices

Particularly for younger students, it is really important that screens are regarded as public screens. That is, they are never used in private places. Not in bedrooms or anywhere out of sight. Dining tables for homework that has to be done online are great, or the lounge room for reading. As students get older you can reduce the amount of intrusion, for example devices may be allowed in the bedroom but the door must be open

Devices up!

Agree on a place for all connected devices to live at night. It might be on a shelf near a power point so charging can happen too but devices should not accompany children to bedrooms at night. The temptation to just see what's happening on Facebook/Instagram/YouTube/Tumblr/Kik/Snapchat etc is just too great! The time for devices up should be no less than 90 minutes before bed. Brain research clearly shows that bright screens cause the secretion of serotonin, a wakefulness hormone in your brain. Literally looking at a screen can keep you awake at night long after you've stopped

Taking control of devices

Technical restrictions

Most routers (the box with all the lights that connect you to the internet) have a capacity for MAC address filtering and control. Every single connected device has a unique MAC address like 8C-70-5A-3D-C6-74. Most good routers can be set to deny and allow connection based on the MAC address of a device and can control the hours that access is allowed between. This isn't hard to setup; a quick Google search if you know the model of your router should return instructions with pictures.

Screen times as currency

Use access to your home network as a currency to trade for time doing activities that offset screen use (preferably that involve physical activity or are outdoors). Why not use this to the advantage of your whole family to encourage some housework help?

Redirection

That initial period where students are becoming accustomed to what are reasonable limits on the device use are really critical. What's established here will determine what happens down the road when students are older and perhaps less receptive to simply following directions, so be prepared to invest some time and effort

Modelling

It's not surprising how unreceptive children can be to ICT use restrictions if they see you as a parent doing exactly what you are restricting them from doing. While we can make very valid arguments that the rules are different for adults, in the break-in period you may find it much easier if you curtail your own use where you can (phones included). Instead try reading a book with or alongside your child – double benefit in that you'll get some quality down time and your child will improve their reading and overall cognitive performance.

Getting outdoors

This could be a great time to invest in some non-passive activities with or for your child. To coincide with this initial period, try and find an activity that your child can do outside of the home. Local council, community groups, churches, sporting clubs and organisations like the CFA run an amazing array of free activities you can look into. Alternatively, you may need to develop a sudden and compelling interest in evening

walking with your child, maybe take the dog! You'll need to persist for a couple of months but, you be healthier, so will your child and maybe the dog.

These are just a few of the strategies you can employ which are tested and effective. The Melba College website under Digital Learning has links to many good online resources for you to find out more.

A quick guide to home internet filtering

There are a number of ways to help control the websites that users of your home network visit.

It must be kept in mind though that none of them are foolproof, and they must be used in conjunction with parental supervision.

It is strongly recommended that when at home iPads and computers in general are not used in locations which are not "public". For example, parents may opt to forbid students from using internet connected devices in their bedrooms or may institute an open bedroom door policy for older children. Ultimately, the decisions are up to parents and to help links to a great deal of very useful reading may be found in this booklet.

Internet filtering – the software option

A common method of filtering the internet content available is to use a software application on each device connected to the internet. This will require each device to be configured and that configuration password protected. There is also a cost to this software that varies according to the product selected.

Here are the most common applications used:

Net Nanny - <https://www.netnanny.com/>

McAfee Family Protection - <http://www.mcafee.com/familyprotection.com/a/>

Norton Family - <https://family.norton.com/web/>

Internet filtering – the free name server option

All sites on the internet are identified by a series of numbers called an IP Address. For example www.google.com.au is 216.58.220.142. A service called a Name Server (known as a DNS) translates the address in words (i.e. google.com.au) to an IP address

and directs your web browser there. Think of it like a telephone book for the internet that you would rarely, if ever, be aware of. However, your router – that’s the box connected to the telephone line that has aerials and flashing lights – has a setting for a DNS provided by your ISP which you can change. Norton Securities provide a free DNS service that filters out sites that are deemed inappropriate, depending on the type of protection you want. They have three options:

A– Protection against malware, phishing sites and scam sites

B– A and pornography

C– A and pornography/other (highest level protection)

The address for the DNS for each level of filtering is provided in the table below (two DNS IP addresses are used by your router in case one fails for any reason).

Changing the DNS is different on every model of router, but is generally not very difficult. Our tech staff can assist you by phone or remote access.

Please email support@melba.vic.edu.au if you need help.

| Option A | Option B | Option C |
|-----------------|-----------------|-----------------|
|-----------------|-----------------|-----------------|

| | | |
|---------------|---------------|---------------|
| 199.85.126.10 | 199.85.126.20 | 199.85.126.30 |
|---------------|---------------|---------------|

| | | |
|---------------|---------------|---------------|
| 199.85.127.10 | 199.85.127.20 | 199.85.127.30 |
|---------------|---------------|---------------|

What to do if things go wrong

With any technology, there will be things that happen that you weren’t expecting, and there will be accidents.

Technical Problems

For problems with how to do a particular task on a device or fix an operating problem, the Student Helpdesk - TECHNIC - is the first place to visit. Some of our student leaders volunteer their own time to help other students with their ICT problems. They are very knowledgeable and eager to help, and can be found at the ICT Support Centre at lunchtimes several days a week. Students will be emailed credentials to access TECHNIC with their connection.

Students can also log their problems on an electronic helpdesk; this creates a virtual job ticket to which the TECHNIC Team will respond by email initially and then in

person if required.

If the TECHNIC Team can't help, then our Senior Technicians are on hand every day to step in and help resolve the issue where possible.

Damage or Loss Problems

If the device was purchased through the Melba/JB Education portal with insurance, parents must contact the Insurance Hotline on **1300 786 225**.

Repairs to externally sourced devices are the responsibility of the student/parent. If damaged, the device must be returned to full functionality as quickly as practicable. Damaged devices are not permitted to stay in use at school.

If a device is under warranty, all repairs must be carried out by an authorised warranty repairer (For Apple devices, this is Apple only) to retain the warranty. For out-of-warranty repairs, the TECHNIC Team can recommend local repairers.

FAQs

If I order a device through the purchase portal when will I receive it?

Orders typically arrive after the second week of January

Why should I order a cover for an iPad or tablet device?

Even dropping an iPad on carpet without a cover can result in expensive damage. The cover saves parents money and students lost learning time

If I am supplying my own device what do I have to do now?

For the parents of new Year 7 students, you should check the email address you registered at Melba College and follow the connection instructions contained inside. You also must make sure you have all the Tier 1 apps installed relevant to the Year level of your child.

For parents of 10 - 12 students, if you child is not already participating in the program from 2017 then they will be connected in person in the first week of term. For any other students returning with a previously connected device it will function and connect as before.

What if I don't order until next year?

You may not receive your device until into the start of term. If your child has opted for an eBook this may cause difficulties from not being able to access the textbook for a subject.

Do I have to buy eBooks instead of printed books?

No. Although they are considerably more expensive, you may opt for a printed book. Second hand copies may be available at school for purchase.

What do I do if I have technical problems at home getting the iPad to connect?

Our TECHNIC Team are happy to offer you advice. They are often engaged in helping students so you may need to leave a message. You can contact them at either campus or at support@melba.vic.edu.au

I'm worried about over-use of technology. What can I do?

First, don't panic. We like students to have their iPad prior to Christmas so that they can get the initial over-enthusiasm out of their system if possible. It is quite normal for students to seem inseparable from the device for the first weeks. Please see the section on [overuse](#)

What if I don't have a credit card?

iPad purchases can be made by direct deposit and iTunes credit can be purchased by purchasing a voucher card - instructions are available in this guide under the [Apple ID section](#)

Where can I get credit for the App Store?

Purchase an iTunes card from any of these stores;

Big W, KMart, Coles Stores , Woolworth Stores, Australia Post, BP Petrol Stations, Coles Express Petrol Stations, Australia Post, 7-11 Stores and Officeworks

Who can I call if I need to discuss something?

The eLearning leader is Mr Brett Groves who is responsible for the ICT Program. You can contact him on 995 555 735. Please don't hesitate to leave a message, your call will be returned. Alternatively, any of the Assistant Principals or sub school leaders can discuss any issues with you.

I want to connect something other than an iPad at Junior levels

Unfortunately, at present this is not possible. We cannot support a range of devices and still ensure their reliability and safety. The iPad has been specified with considerable forethought and the College's long experience with one-to-one ICT.

I'm worried about my child being online. What can I do?

Please make sure you attend either of the Term 1 2019 Cyber Safety Sessions for parents. Keep up with the @melba blog at

<http://melba.vic.edu.au/learning/digital-learning/melba-cybersafety-blog/>

or follow the links from the Melba website.