Department of Education and Training

Dalby State School

Computer Handbook

Queensland Government

Contents

Personally-owned laptop charter

BYOL overview

Bring Your Own Laptop (BYOL) is a new pathway supporting the delivery of 21st century learning. It is a term used to describe a digital device ownership model where students or staff use their personally-owned laptop to access the department's information and communication (ICT) network.

Access to the department's ICT network is provided only if the laptop meets the department's security requirements which, at a minimum, requires that anti-virus software has been installed, is running and is kept updated on the device Advice for State Schools on Acceptable use of ICT Facilities and Devices.

Students and staff are responsible for the security, integrity, insurance and maintenance of their personal laptops and their private network accounts.

The BYOL acronym used by Dalby State School refers to the teaching and learning environment in Queensland state schools where personally-owned laptops are used. The 'L' in BYOL represents more than a personally – owned laptop, it also includes software, applications, connectivity or carriage services.

We have chosen to support the implementation of a BYOL model because:

- BYOL recognises the demand for seamless movement between school, work, home and play
- our BYOL program assists students to improve their learning outcomes in a contemporary educational setting
- assisting students to become responsible digital citizens enhances the teaching learning process and achievement of student outcomes as well as the skills and experiences that will prepare them for their future studies and careers.

Laptop selection

Before acquiring a laptop to use at school the parent or caregiver and student should be aware of the school's specification of appropriate laptop types, operating system requirements and software. These specifications relate to the suitability of the laptop to enable class activities, meeting student needs and promoting safe and secure access to the department's network.

Dalby State School's computer programs may support printing, filtered internet access, and file access and storage through the department's network while at school. However, the school's Computer program's do not include school technical support or charging of devices at school.

Specifications	Minimum Requirements
Processor (CPU)	Intel Core i5
RAM	8GB
Wireless	5GHz Wifi + Bluetooth
Hard Drive	500GB HDD or 256GB SSD
Operating System	Windows 10
External Ports	2 USB, Audio & Ethernet (RJ45)
Warranty	3 Years

Additional Notes:

- Student **MUST** be an Administrator for that Device
- Anti-virus **MUST** be installed
- Students need to have Microsoft Office installed- Can download for free on learning place
- DVD Drive (Optional)
- Wired Mouse (Optional)
- Headphones
- Carry bag to suit (Backpack preferred)
- The above specifications are in line with High School Laptop requirements allowing for easy transition between schools
- Gaming software such as Steam is not to be installed on this device as it causes issues with the BYOx installation and software.

Laptop care

The student is responsible for taking care of and securing the laptop and accessories in accordance with school policy and guidelines. Responsibility for loss or damage of a laptop at home, in transit or at school belongs to the student. Advice should be sought regarding inclusion in home and contents insurance policy.

It is advised that accidental damage and warranty policies are discussed at point of purchase to minimise financial impact and disruption to learning should a laptop not be operational.

General precautions

- Food or drink should never be placed near the laptop.
- Plugs, cords and cables should be inserted and removed carefully.
- Laptops should be carried within their protective case where appropriate.
- Carrying laptops with the screen open should be avoided.
- Ensure the battery is fully charged each day.
- Turn the laptop off before placing it in its bag.

Protecting the screen

- Avoid poking at the screen — even a touch screen only requires a light touch.
- Don't place pressure on the lid of the laptop when it is closed.
- Avoid placing anything on the keyboard before closing the lid.
- Avoid placing anything in the carry case that could press against the cover.
- Only clean the screen with a clean, soft, dry cloth or an anti-static cloth.
- Don't clean the screen with a household cleaning product.

Data security and back-ups

Students must ensure they have a process of backing up data securely. Otherwise, should a hardware or software fault occur, assignments and the products of other class activities may be lost.

The student is responsible for the backup of all data. While at school, students may be able to save data to the school's network, which is safeguarded by a scheduled backup solution. All files must be scanned using appropriate anti-virus software before being downloaded to the department's ICT network.

Students are also able to save data locally to their device for use away from the school network. The backup of this data is the responsibility of the student and should be backed-up on an external device, such as an external hard drive or USB drive.

Students should also be aware that, in the event that any repairs need to be carried out the service agents may not guarantee the security or retention of the data. For example, the contents of the device may be deleted and the storage media reformatted.

Acceptable personal laptop use

Upon enrolment in a Queensland Government school, parental or caregiver permission is sought to give the student(s) access to the internet, based upon the policy contained within the Acceptable Use of the Department's Information, Communication and Technology (ICT) Network and Systems

This policy also forms part of this Student Laptop Charter. The acceptable-use conditions apply to the use of the laptop and internet both on and off the school grounds.

Communication through internet and online communication services must also comply with the department's Code of School Behaviour and the Responsible Behaviour Plan available on the school website.

While on the school network, students should not:

- create, participate in or circulate content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disable settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- use unauthorised programs and intentionally download unauthorised software, graphics or music
- intentionally damage or disable computers, computer systems, school or government networks
- use the laptop for unauthorised commercial activities, political lobbying, online gambling or any unlawful purpose.

Note: Students' use of internet and online communication services may be audited at the request of appropriate authorities for investigative purposes surrounding inappropriate use.

Passwords

Use of the school's ICT network is secured with a user name and password. The password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students).

The password should be changed regularly, as well as when prompted by the department or when known by another user.

Personal accounts are not to be shared. Students should not allow others to use their personal account for any reason.

Students should log off at the end of each session to ensure no one else can use their account or laptop.

Students should also set a password for access to their BYOL and keep it private.

Parents/caregivers may also choose to maintain a password on a personally-owned laptop for access to the laptop in the event their student forgets their password or if access is required for technical support. Some laptops may support the use of parental controls with such use being the responsibility of the parent/caregiver.

Digital citizenship

Students should be conscious creators of the content and behaviours they exhibit online and take active responsibility for building a positive online reputation. They should be conscious of the way they portray themselves, and the way they treat others online.

Students should be mindful that the content and behaviours they have online are easily searchable and accessible. This content may form a permanent online record into the future.

Interactions within digital communities and environments should mirror normal interpersonal expectations and behavioural guidelines, such as when in a class or the broader community.

Parents are requested to ensure that their child understands this responsibility and expectation. The school's Responsible Behaviour Plan also supports students by providing school related expectations, guidelines and consequences.

Cybersafety

If a student believes they have received a computer virus, spam (unsolicited email), or they have received a message or other online content that is inappropriate or makes them feel uncomfortable, they must inform their teacher, parent or caregiver as soon as is possible.

Students must also seek advice if another user seeks personal information, asks to be telephoned, offers gifts by email or asks to meet a student.

Students are encouraged to explore and use the 'Cybersafety Help button' to talk, report and learn about a range of cybersafety issues.

Students must never initiate or knowingly forward emails, or other online content, containing:

- a message sent to them in confidence
- a computer virus or attachment that is capable of damaging the recipients' computer
- chain letters or hoax emails
- spam (such as unsolicited advertising).

Students must never send, post or publish:

- inappropriate or unlawful content which is offensive, abusive or discriminatory
- threats, bullying or harassment of another person
- sexually explicit or sexually suggestive content or correspondence
- false or defamatory information about a person or organisation.

Parents, caregivers and students are encouraged to read the department's Cybersafety and Cyberbullying guide for parents and caregivers.

Web filtering

The internet has become a powerful tool for teaching and learning, however students need to be careful and vigilant regarding some web content. At all times students, while using ICT facilities and devices, will be required to act in line with the requirements of the *Code of School Behaviour*) and any specific rules of the school. To help protect students (and staff) from malicious web activity and inappropriate websites, the school operates a comprehensive web filtering system. Any device connected to the internet through the school network will have filtering applied.

The filtering system provides a layer of protection to staff and students against:

- inappropriate web pages
- spyware and malware
- peer-to-peer sessions
- scams and identity theft.

This purpose-built web filtering solution takes a precautionary approach to blocking websites including those that do not disclose information about their purpose and content. The school's filtering approach represents global best-practice in internet protection measures. However, despite internal departmental controls to manage content on the internet, illegal, dangerous or offensive information may be accessed or accidentally displayed. Teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student.

Students are required to report any internet site accessed that is considered inappropriate. Any suspected security breach involving students, users from other schools, or from outside the Queensland DET network must also be reported to the school.

The personally-owned devices have access to home and other out of school internet services and those services may not include any internet filtering. Parents and caregivers are encouraged to install a local filtering application on the student's laptop for when they are connected in locations other than school. Parents/caregivers are responsible for appropriate internet use by students outside the school.

Parents, caregivers and students are also encouraged to visit the Australian Communications and Media Authority's CyberSmart website for resources and practical advice to help young people safely enjoy the online world.

Privacy and confidentiality

Students must not use another student or staff member's username or password to access the school network or another student's laptop, including not trespassing in another person's files, home drive, email or accessing unauthorised network drives or systems.

Additionally, students should not divulge personal information via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school. It is important that students do not publish or disclose the email address of a staff member or student without that person’s explicit permission. Students should also not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others. They should ensure that privacy and confidentiality is always maintained.

Intellectual property and copyright

Students should never plagiarise information and should observe appropriate copyright clearance, including acknowledging the original author or source of any information, images, audio etc. used. It is also important that the student obtain all appropriate permissions before electronically publishing other people’s works or drawings. The creator or author of any material published should always be acknowledged. Material being published on the internet or intranet must have the approval of the principal or their delegate and have appropriate copyright clearance.

Copying of software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

Software

Schools may recommend software applications in order to meet the curriculum needs of particular subjects. Parents/caregivers may be required to install and support the appropriate use of the software in accordance with guidelines provided by the school. This includes the understanding that software may need to be removed from the device upon the cancellation of student enrolment, transfer or graduation.

Monitoring and reporting

Students should be aware that all use of internet and online communication services can be audited and traced to the account of the user.

All material on the laptop is subject to audit by authorised school staff. If at any stage there is a police request, the school may be required to provide the authorities with access to the laptop and personal holdings associated with its use.

Misuse and breaches of acceptable usage

Students should be aware that they are held responsible for their actions while using the internet and online communication services. Students will be held responsible for any breaches caused by other person(s) knowingly using their account to access internet and online communication services.

The school reserves the right to restrict/remove access of personally owned laptops to the intranet, internet, email or other network facilities to ensure the integrity and security of the network and to provide a safe working and learning environment for all network users. The misuse of personally owned laptops may result in disciplinary action which includes, but is not limited to, the withdrawal of access to school supplied services.

Responsible use of BYOL

Our goal is to ensure the safe and responsible use of facilities, services and resources available to students through the provision of clear guidelines.

Responsibilities of stakeholders involved in the BYOL program:

School

- Computer program induction — including information on (but not responsible for) connection, care of device at school, workplace health and safety, appropriate digital citizenship and cybersafety
- network connection at school
- internet filtering (when connected via the school's computer network)
- some technical support (please consult Technical support table below)
- some school-supplied software e.g. Adobe, Microsoft Office 365 …
- printing facilities
- school representative signing of BYOL Charter Agreement.

Student

- participation in relevant computer program induction
- acknowledgement that core purpose of device at school is for educational purposes
- care of device
- appropriate digital citizenship and online safety (for more details, see ACMA CyberSmart)
- security and password protection — password must be difficult enough so as not to be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students)
- some technical support (please consult Technical support table below)
- maintaining a current back-up of data
- charging of laptop
- abiding by intellectual property and copyright laws (including software/media piracy)
- internet filtering (when not connected to the school's network)

- ensuring personal login account will not be shared with another student, and laptop will not be shared with another student for any reason
- understanding and signing the BYOL Charter Agreement.

Parents and caregivers

- participation in relevant computer program induction
- acknowledgement that core purpose of device at school is for educational purposes
- internet filtering (when not connected to the school's network)
- encourage and support appropriate digital citizenship and cybersafety with students (for more details, see ACMA CyberSmart)
- some technical support (please consult Technical support table below)
- required software, including sufficient anti-virus software
- protective backpack or case for the device
- adequate warranty and insurance of the device
- understanding and signing the BYOL Charter Agreement.

Technical support

	Connection:	Hardware:	Software:
Parents and Caregivers	✓ (home-provided internet connection)	✓	✓
Students	✓	✓	✓
School	✓ school provided internet connection	(dependent on school-based hardware arrangements)	✓ (some school-based software arrangements)
Device vendor		✓ (see specifics of warranty on purchase)	

The following are examples of responsible use of laptops by students:

- Use laptops for:
  - engagement in class work and assignments set by teachers
  - developing appropriate 21st Century knowledge, skills and behaviours
  - authoring text, artwork, audio and visual material for publication on the Intranet or Internet for educational purposes as supervised and approved by school staff
  - conducting general research for school activities and projects
  - communicating or collaborating with other students, teachers, parents, caregivers or experts as part of assigned school work
  - accessing online references such as dictionaries, encyclopaedias, etc.
  - researching and learning through the school's eLearning environment
  - ensuring the device is fully charged before bringing it to school to enable continuity of learning.

- Be courteous, considerate and respectful of others when using a laptop.
- Switch off and place out of sight the laptop during classes, where these laptops are not being used in a teacher directed activity to enhance learning.
- Use the personal laptop for private use before or after school, or during recess and lunch breaks.
- Seek teacher's approval where they wish to use a laptop under special circumstances.

The following are examples of irresponsible use of laptops by students:

- using the laptop in an unlawful manner
- creating, participating in or circulating content that attempts to undermine, hack into and/or bypass the hardware and/or software security mechanisms that are in place
- disabling settings for virus protection, spam and/or internet filtering that have been applied as part of the school standard
- downloading (or using unauthorised software for), distributing or publishing of offensive messages or pictures
- using obscene, inflammatory, racist, discriminatory or derogatory language
- using language and/or threats of violence that may amount to bullying and/or harassment, or even stalking
- insulting, harassing or attacking others or using obscene or abusive language
- deliberately wasting printing and Internet resources
- intentionally damaging any laptops, accessories, peripherals, printers or network equipment
- committing plagiarism or violate copyright laws
- using unsupervised internet chat
- sending chain letters or spam email (junk mail)
- accessing private 3G/4G networks during lesson time
- knowingly downloading viruses or any other programs capable of breaching the department’s network security
- using the laptops camera anywhere a normal camera would be considered inappropriate, such as in change rooms or toilets
- invading someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- using the laptop (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use laptops at exams or during class assessment unless expressly permitted by school staff.

In addition to this:

Information sent from our school network contributes to the community perception of the school. All students using our ICT facilities are encouraged to conduct themselves as positive ambassadors for our school.

- Students using the system must not at any time attempt to access other computer systems, accounts or unauthorised network drives or files or to access other people's devices without their permission and without them present.

- Students must not record, photograph or film any students or school personnel without the express permission of the individual/s concerned and the supervising teacher.

- Students must get permission before copying files from another user. Copying files or passwords belonging to another user without their express permission may constitute plagiarism and/or theft.

- Students need to understand copying of software, information, graphics, or other data files may violate copyright laws without warning and be subject to prosecution from agencies to enforce such copyrights.

- Parents and caregivers need to be aware that damage to laptops owned by other students or staff may result in significant consequences in relation to breaches of expectations and guidelines in the school's Responsible Behaviour Plan.

- The school will educate students on cyber bullying, safe internet and email practices and health and safety regarding the physical use of electronic devices. Students have a responsibility to incorporate these safe practices in their daily behaviour at school.

The school's BYOL program supports personally-owned laptops in terms of access to:

- printing
- internet
- file access and storage
- support to connect devices to the school network.

However, the school's BYOL program does not support personally-owned laptops in regard to:

- technical support
- charging of devices at school
- security, integrity, insurance and maintenance
- private network accounts.

BYOL FAQ's

Q: What is BYOL?
A: *BYOL stands for "Bring Your Own Device." BYOL is an initiative that will allow students who have personal technology devices to bring them to school, to use them for educational purposes to meet their learning needs under the direction of a teacher.*

Q: What are the benefits of BYOL?
A: *Our students are living in a world where they have immediate access to information anytime and anywhere. Many students' have personally-owned devices that can be used to allow them to learn in their own style and at their own pace. With digital learning, every student can access high quality and rigorous instruction, thereby maximising their opportunity for success in school and beyond. Specific Benefits include:*

- *Allowance for personalised learning*
- *Improved student learning outcomes*
- *Improved collaboration*
- *Give student greater choice and more independence*
- *It creates a model for lifelong learning*
- *Smooth transition between home and school*
- *Allows 24/7/365 access*
- *Provides easier student access to online instructional materials*
- *Supplements school resources and equipment*
- *Normalisation of technology*

Q: Why only allow laptops?
A: *We believe in a consistent approach to ensure best productivity with regards to maximising student learning outcomes.*

Q: Why not allow BYOL across the whole school?
A: *At Dalby State School, we want to ensure that both teachers and students are best prepared to achieve the best possible outcomes from teachers and students alike.*

Q: Will I be expected to purchase a new laptop and do I have to purchase from a particular store e.g. Dell, HP?
A: *No, you can choose to use a laptop that you already own or purchase a new laptop. No, we will not recommend a store where you can purchase a laptop; however, we can provide details of providers. We do not endorse any one store.*

Q: Should we purchase a carry case for the laptop and if so, which one should we buy?
A: *Yes, you should purchase a carry case. We recommend that the carry case should protect both the front and back of the laptop. We will not recommend a store where you can purchase a case or cover. We do not endorse any one store.*

Q: Will the BYOL classes be made up of a particular group of students e.g. academic, SEP etc.?
A: *No, the make-up of BYOL classes for 2018 will have the same considerations as the non-BYOL classes. Considerations include, but are not limited to, academic and gender balance across classes, consideration of parent requests etc.*

Q: Will students use their laptop in class on a day that the regular class teacher is away?
A: *Yes.*

Q: Can my child bring a 3G enabled laptop without the SIM?
A: *Yes. The reason why we do not want external controlled Internet access is that by the students going through our school wireless, they are also going through Education Queensland Internet filters, helping protect our students from accessing inappropriate content.*

Q: Are we required to purchase a stylus pen?
A: *Yes, if you purchase a laptop with touch screen possibilities.*

Q: Will my child require a username and password?
A: *Yes. It is a departmental requirement that a username and password is used to access the school network. This is provided by the school.*

Q: My child has a laptop at home already. Will that laptop be suitable for use at school?
A: *Any laptop that meets the minimum specifications for the BYOL program is suitable for use at school. These specifications will be communicated at the parent information evening.*

Q: Where can I purchase a suitable laptop?
A: *Laptops can be purchased from a range of retailers. However, the school has established portals with various suppliers to provide devices to parents that meet the minimum requirements for the school's BYOL program. The portals (or supply arrangements) that the school offers provide commercial grade laptops, with commercial grade warranty conditions. As the school has existing relationships with most of the suppliers that are offering portals or supply arrangements, this can facilitate faster repairs.*

Q: What happens if a student uses a laptop inappropriately?
A: *The Acceptable Use Policy and Behaviour Policy will outline the sanctions for inappropriate use of laptops and network. Students and their parents will be required to sign agreements that these policies will be adhered to and that consequences of policy breaches are understood before network access is provided.*

Q: What about security, theft and damage to the laptop?
A: *Laptops will be the responsibility of the student and laptops will be stored in classrooms during class time and at break time. Students will be educated in the proper care and appropriate use of their laptop. Parents will be advised to review their insurance policies to ensure that BYOL is covered outside the home, and to provide a suitable protective bag for the laptop. The school will accept no responsibility for the security or safety of the laptop.*

Q: Do I need a warranty?
A: *We strongly recommend that all laptops have some form of extended warranty. While research shows that students take much better care of a laptop which belongs to them than a school provided laptop, accidents happen.*

Q: What is the policy for charging personally owned laptops while at school?
A: *It is expected that personally owned laptops are brought into school with a full charge. Students will be made aware that the school is not responsible to provide an opportunity or the necessary power to charge their laptop during the school day.*

Q: What is the policy for printing from personally owned laptops?
A: *Students will be able to access printing at school with a teacher's permission*

Q: How much of the time will students be using their own laptop?
A: *Teachers will direct students to use laptops where they are the best tool for learning. This will vary between year groups and subjects studies.*

Q: What training will be provided to students?
A: *As part of the BYOL program students will undergo training on the Acceptable Use Policy and the changes which have been introduced in the light of BYOL will be highlighted and reinforced. Students will also receive training on; file management tips and techniques, referencing and academic honesty, health and safety when using electronic devices, cyberbullying, plus anything else which the school deems appropriate.*

Q: Who can I contact for further information?
A: *Please contact the school office on 4672 3666 or admin@dalbyss.eq.edu.au for further information.*

Q: What is "Onboarding"?
A: *Onboarding is the technical term used to describe the procedure that students need to perform to get their laptops operational on the school network. Dalby State School uses a system that allows safe, secure, and largely automatic onboarding for most laptops, and information about the use of this system will be provided to students when they join the BYOL program. If students require any assistance with onboarding their laptop, they are free to contact the school's ICT Support.*

Q: Will all students have the same laptop, and if not, how will this affect learning in the classroom?
A: *Not all students will have the same laptop – many of them will differ in size, type, input method and operating system. In order to minimise the impact that this will have on learning in the classroom, parents are encouraged to purchase using the supply arrangements that we have established so that there are "common" laptops that will work with the school's network. The use of these "common" laptops will ensure the greatest access to the range of curriculum software used at Dalby State School, with most curriculum software used by teachers made available to BYOL users for free from the school over a wide range of operating systems.*

Q: Will the school assist me with home internet connection settings, or issues?
A: *This is not part of the support offered by the school. The school's support is limited to providing assistance with onboarding the laptop to the network and curriculum related inquiries. If you require assistance for personal issues regarding your laptop, your home internet service provider or private computer technician should be able to assist with these enquiries.*

Q: Do students need to backup the data stored on their laptop?
A: *Backup of laptop data is the student's responsibility. Work that is completed at school can be saved to the school's servers. However, work completed at home or stored on the laptop will need to be backed up in case the laptop encounters a problem such as a hardware failure.*

Q: How will students be kept safe online?
A: *Access to the Internet at school is filtered. As part of the curriculum, students are instructed on Cyber safety. At home, it is the parent/guardian's responsibility to ensure any appropriate content filters or controls are applied to internet services. The school accepts no responsibility for consequences of internet access outside the school.*

Q: What should I consider if I am purchasing a new laptop?

- *Specifications – minimum specifications will be provided at the parent information session*
- *Life of the device – consider the length of time you require the device to service the needs of your family*
- *Add-ons – beware of adding unnecessary additional features as this will increase the price of the device*
- *Length of warranty – extending the warranty to 3-4 years is advisable*
- *Warranty conditions – consider what the warranty covers (read the fine print)*
- *Personal contents insurance – determine if this covers laptop/digital device damage*
- *Cost of repairs – screen and keyboard are the most commonly damaged parts*

Free and Cheap Software - Where to get it……

Office 365

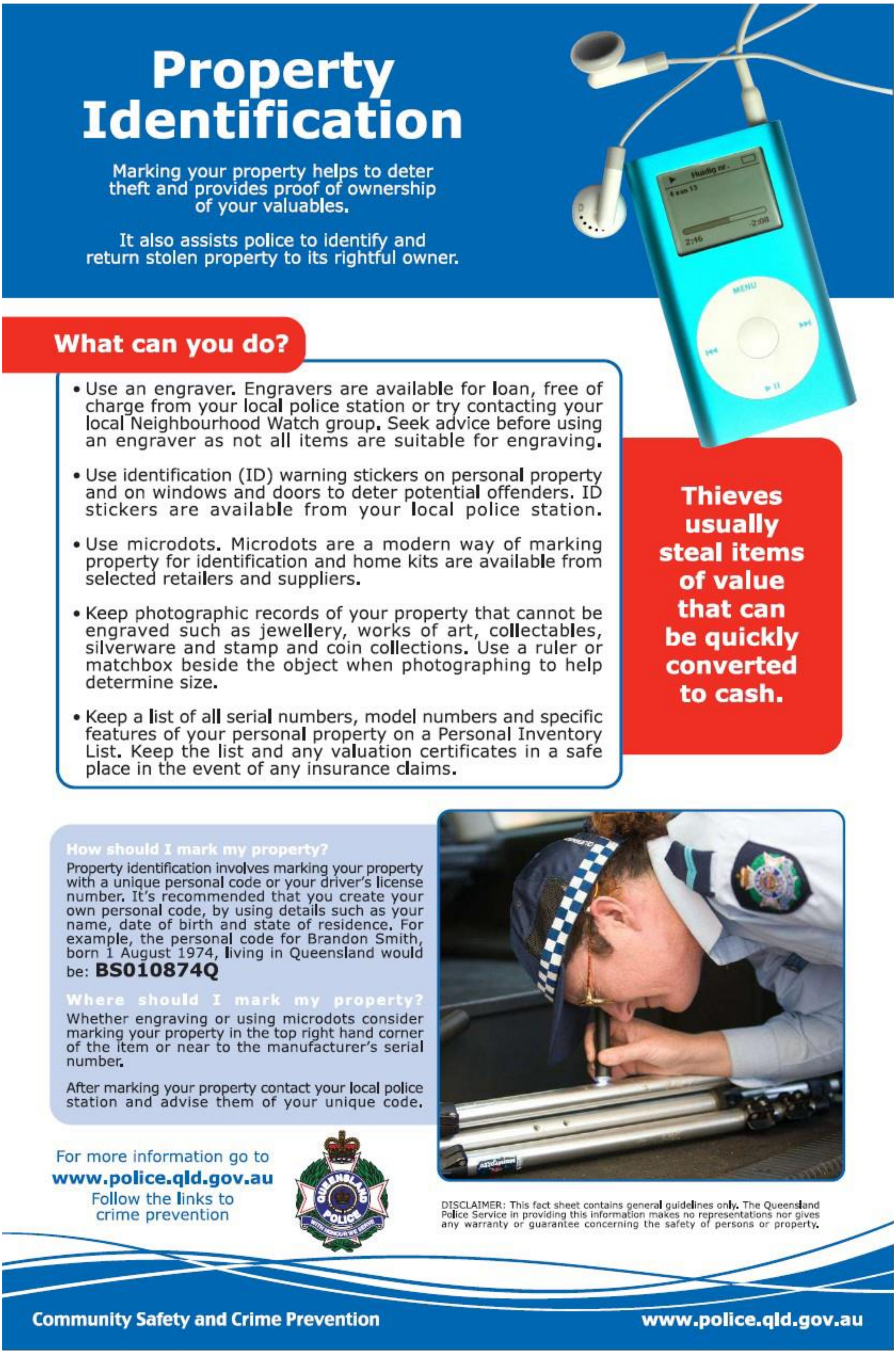
http://portal.microsoft.com

Norton by Symantec

https://phoenix.symantec.com/DETE/index.php?offercode=qlddete14

Norton Security with Backup for 1 Device 1 Year Protection @ $9.99
Norton Security with Backup for 1 Device 3 Years Protection @ $29.99

AUTODESK. http://www.autodesk.com/education/free-software/all



Property Identification

Marking your property helps to deter theft and provides proof of ownership of your valuables.

It also assists police to identify and return stolen property to its rightful owner.

What can you do?

- Use an engraver. Engravers are available for loan, free of charge from your local police station or try contacting your local Neighbourhood Watch group. Seek advice before using an engraver as not all items are suitable for engraving.
- Use identification (ID) warning stickers on personal property and on windows and doors to deter potential offenders. ID stickers are available from your local police station.
- Use microdots. Microdots are a modern way of marking property for identification and home kits are available from selected retailers and suppliers.
- Keep photographic records of your property that cannot be engraved such as jewellery, works of art, collectables, silverware and stamp and coin collections. Use a ruler or matchbox beside the object when photographing to help determine size.
- Keep a list of all serial numbers, model numbers and specific features of your personal property on a Personal Inventory List. Keep the list and any valuation certificates in a safe place in the event of any insurance claims.

Thieves usually steal items of value that can be quickly converted to cash.

How should I mark my property?

Property identification involves marking your property with a unique personal code or your driver's license number. It's recommended that you create your own personal code, by using details such as your name, date of birth and state of residence. For example, the personal code for Brandon Smith, born 1 August 1974, living in Queensland would be: **BS010874Q**

Where should I mark my property?

Whether engraving or using microdots consider marking your property in the top right hand corner of the item or near to the manufacturer's serial number.

After marking your property contact your local police station and advise them of your unique code.

For more information go to
www.police.qld.gov.au
Follow the links to
crime prevention

DISCLAIMER: This fact sheet contains general guidelines only. The Queensland Police Service in providing this information makes no representations nor gives any warranty or guarantee concerning the safety of persons or property.

Community Safety and Crime Prevention **www.police.qld.gov.au**