

This document needs to be carefully read and signed by the student, parent/caregiver and a school representative.



# Miles State HIGH SCHOOL

Strive to Achieve'

## Student ICT Agreement Acceptable Use of Technology

STUDENT'S  
NAME:

YEAR:

*Experience a Supportive Community ...*

*Experience Academic Success ...*

*Experience Sporting Excellence ...*

*Experience Your Future ...*

**RESPECT**

**INTEGRITY**

**SAFETY**

**ENGAGE**

## Contents

<b>Loan equipment .....</b>	<b>3</b>
<b>Equipment ownership .....</b>	<b>3</b>
<b>Standard ICT Package .....</b>	<b>3</b>
<b>Device care .....</b>	<b>4</b>
<b>Data security and back ups .....</b>	<b>4</b>
<b>Miles State High School Information Communication Technology Policies .....</b>	<b>4</b>
<b>Acceptable Computer and Internet Use .....</b>	<b>4</b>
<b>PASSWORDS .....</b>	<b>5</b>
<b>CYBERSAFETY .....</b>	<b>5</b>
<b>WEB FILTERING .....</b>	<b>5</b>
<b>PRIVACY AND CONFIDENTIALITY .....</b>	<b>5</b>
<b>INTELLECTUAL PROPERTY AND COPYRIGHT .....</b>	<b>5</b>
<b>MISUSE AND BREACHES OF ACCEPTABLE USAGE .....</b>	<b>6</b>
<b>DAMAGE OR LOSS OF EQUIPMENT .....</b>	<b>6</b>
<b>WILFUL AND MALICIOUS DAMAGE .....</b>	<b>6</b>
<b>Acceptable use of Social Media .....</b>	<b>6</b>
<b>ROLE OF SOCIAL MEDIA .....</b>	<b>7</b>
<b>APPROPRIATE USE OF SOCIAL MEDIA .....</b>	<b>7</b>
<b>LAW AND CONSEQUENCE OF INAPPROPRIATE ONLINE BEHAVIOUR AND CYBERBULLYING .....</b>	<b>7</b>
<b>Software Monitoring and Reporting .....</b>	<b>8</b>
<b>SOFTWARE .....</b>	<b>8</b>
<b>MONITORING AND REPORTING ON SCHOOL NETWORKS .....</b>	<b>8</b>
<b>STUDENTS' REPORTING REQUIREMENTS .....</b>	<b>8</b>

## Loan equipment

The equipment referred to in this charter are the devices that have been purchased by the school and consists of a desktop or a laptop computer and power pack and DoE's standard suite of software, including Microsoft Office.

Each device is:

- protected by anti-virus tools and automated updates
- covered by a four year warranty
- covered by accidental damage protection (excess applies)
- connected to the school network and have filtered internet and email
- installed with DoE's standard suite of productivity software

## Equipment ownership

At the end of the loan period, all devices (laptop, desktop or tablet) will be formatted and reimaged. This means ALL data will be permanently deleted from the device. Please refer to page 4 of the Student ICT Charter for information pertaining to the backing up of student's data within DoE.

It is also a requirement of using the device that students provide authorised school staff with access to the device and personal holdings associated with the use of the device if requested.

## Standard ICT Package

The items below are included in Queensland's standard ICT package:

Device item	Annual cost per student
ICT device desktop/laptop	Included
Internet filtering	Included
Windows 10 operating system	Included
Microsoft Office software suite	Included
Antivirus software	Included

## Device care

The student is responsible for taking care of and securing the device and accessories in accordance with school policy and guidelines.

## Data security and back ups

Students must understand the importance of backing up data securely. Should a hardware or software fault develop, assignment work that has taken a considerable time to prepare may be lost.

The student is responsible for the backup of all data. While at school, students are able to save data to the school's network which is safeguarded by a scheduled backup solution. They are also able to save data locally to a USB to continue their studies at home. The backup of this data is the responsibility of the student and should be backed-up on an external device, such as external hard drive or USB stick. I understand that all memory devices, including USB's, may be checked by school staff at any time.

# Miles State High School Information Communication Technology Policies

## Acceptable Computer and Internet 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 ICT-PR-004 Using the Department's Corporate ICT Network.

This policy also forms part of this Student ICT Device Charter. The acceptable-use conditions apply to the use of the device and internet.

Communication through internet and online communication services must comply with the Responsible Behaviour Plan available on the school website.

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 or Queensland DoE networks use the device 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

Passwords must not be obvious or easily guessed; they must be kept confidential, and changed when prompted or when known by another user. Personal accounts cannot 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.

## CYBERSAFETY

At any time, if a student believes they have received a computer virus or spam (unsolicited email), or they have received a message that is inappropriate or makes them feel uncomfortable, they must inform their teacher as soon as is possible.

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

Students must seek advice if another user seeks personal information, asks to be telephoned, offers gifts by email or asks to meet a student. Students must never initiate or knowingly forward emails, or other messages, 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 or publish:
- Unacceptable or unlawful material or remarks, including offensive, abusive or discriminatory comments
- Threats, bullying or harassment of another person
- Sexually explicit or sexually suggestive material or correspondence  
False or defamatory information about a person or organisation.

## WEB FILTERING

An internet filtering solution provides DoE with the ability to restrict access to inappropriate material on DoE's ICT network.

Content filtering is active 100% of the time on the Computer for Student (CFS) devices. The filtering system is installed on each device.

## PRIVACY AND CONFIDENTIALITY

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.

The student should not reveal personal information including names, addresses, photographs, credit card details or telephone numbers of themselves or others.

It should also be ensured that privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interest.

## INTELLECTUAL PROPERTY AND COPYRIGHT

Students should never plagiarise information and shall observe appropriate copyright clearance, including acknowledging the original author or source of any information 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.

### 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 misuse of internet and online communication services may result in disciplinary action which includes, but is not limited to, the withdrawal of access to services.

### DAMAGE OR LOSS OF EQUIPMENT

All devices and batteries are covered by a manufacturer's warranty which covers manufacturing defects through normal usage. In addition, devices are covered by an insurance policy which protects against accidental damage. There is no cover for negligence, abuse or malicious damage.

Costs incurred by the school for the repair or replacement of devices may be charged by the school as an excess to parents. In the event of non-compliance of agreed responsibilities, schools may review the student's continued participation.

Any software or hardware issues, vandalism or damage to the device must be reported immediately to the teacher/school.

### WILFUL AND MALICIOUS DAMAGE

Where a device is intentionally damaged, parents will be notified of the event, followed by an investigation.

Where the school determines that damage has been intentionally caused to a device or a student has disrespected school property, parents will be invoiced according to the following;

- Lost Case \$10
- Missing keys on keyboard \$30 Broken Screen \$100
- Broken device and not work working \$100

The software loaded on the device is licensed to the DoE or the school.

### Acceptable use of Social Media

Miles State High School embraces the amazing opportunities that technology and the internet provide to students for learning, being creative and socialising online. Use of online communication and social media sites and apps can provide positive social development experiences through an opportunity to develop friendships and shape identities.

When used safely, social media sites and apps such as Facebook, Twitter and Instagram can provide positive opportunities for social learning and development. However, inappropriate, or misguided use can lead to negative outcomes for the user and others.

Miles State High School is committed to promoting the responsible and positive use of social media sites and apps.

No student at Miles State High School will face disciplinary action for simply having an account on Facebook or other social media site.

Any form of Bullying (including Cyberbullying), Racism, Harassment or Victimisation, is unacceptable on the Miles State High School grounds or while online. Inappropriate online behaviours can have a negative impact on student learning and the good order and management of Miles State High School – whether those behaviours occur during or outside of school hours. It is important for students at Miles State High School to engage in appropriate online behaviour.



## ROLE OF SOCIAL MEDIA

The majority of young people use social media and apps on a daily basis for school work, entertainment and to keep in contact with friends. Unfortunately, some young people misuse social media technologies and engage in cyberbullying.

Social media, by its nature, will result in the disclosure and sharing of personal information. By signing up for a social media account, users are providing their personal information.

Students need to remember that the internet is a free space and many social media sites and apps, like Twitter, have limited restrictions placed upon allowable content and regulated procedures for the removal of concerning posts.

Social media site and apps are designed to share online content widely and rapidly.

Once students place information and/or pictures online, they have little to no control over how that content is used. The internet reaches a global audience. Even if students think that the comments or photos have been deleted, there can be archived records of the material that will continue to be searchable into the future.

Inappropriate online behaviour has the potential to embarrass and affect students, others and the school for years to come.

## APPROPRIATE USE OF SOCIAL MEDIA

Students at Miles State High School are expected to engage in the appropriate use of social media. Specific examples of appropriate use of social media sites and apps include: Ensuring that all personal information, such as full name, address, phone number, school name and location and anyone else's personal information, is not shared.

Thinking about what they say or post, and how it could be interpreted by others, before putting it online.

Remember, once content is posted online you lose control over it. Students should not post content online that they would be uncomfortable saying or showing to their parent/carers faces or shouting in a crowded room.

Remember that it can be difficult to work out whether a message typed on social media sites and apps are meant to be funny or sarcastic. Tone of voice and context is often lost which can lead to unintended consequences. If students think a message may be misinterpreted, they should be cautious and make the decision not to post it.

Never provoking, or engaging with, another user who is displaying inappropriate or abusive behaviour. There is no need to respond to a cyberbully. Students should report cyberbullying concerns to a teacher and allow the teacher to record and deal with online concern.

If inappropriate online behaviour impacts on the good order and management of Miles State High School, the school may impose disciplinary consequences for that behaviour regardless of whether the behaviour occurs during or outside of school hours.

Disciplinary consequences could include suspension and/or exclusion. In serious cases of inappropriate online behaviour, the school may also make a report to the police for further investigation.

Miles State High School will not become involved in concerns of cyberbullying or inappropriate online behaviour where the incident in question does not impact upon the good order and management of the school. For example, where cyberbullying occurs between a student of this school and a student of another school outside school hours. Such an incident will be a matter for parents/carers and/or police to resolve.

## LAW AND CONSEQUENCE OF INAPPROPRIATE ONLINE BEHAVIOUR AND CYBERBULLYING

Inappropriate online behaviour may in certain circumstances constitute a criminal offence. Both the Criminal Code Act 1995 (Cth) and the Criminal Code Act 1899 (Qld) contain relevant provisions applicable to cyberbullying.

The Commonwealth Criminal Code outlines a number of criminal offences concerning telecommunications services. The most relevant offence for cyberbullying is “using a carriage service to menace, harass or cause offence to another person”.

The Queensland Criminal Code contains several applicable sections for cyberbullying. Potential relevant criminal offences are

- Unlawful stalking
- Computer hacking and misuse Possession of child exploitation material
- Involving a child in making child exploitation material Making child exploitation material
- Distribution of child exploitation material Criminal Defamation

There are significant penalties for these offences.

Miles State High School strives to create positive environments for all students at all times of the day, including while online. To help in achieving this goal, Miles State High School expects its students to engage in positive online behaviours.

## Software Monitoring and Reporting

### SOFTWARE

Devices may be audited by a school. Devices may be rebuilt at any time for numerous reasons without consultation with students or parents and all local data may be lost in this process.

To stop any malicious software or virus’s entering the DoE network, Miles State High School prohibits the installation of any software or program onto any school device that is licensed to the school or DoE.

### MONITORING AND REPORTING ON SCHOOL NETWORKS

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

### STUDENTS’ REPORTING REQUIREMENTS

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 Queensland DoE must also be reported to the school.



# How to report cyberbullying material

| 1

**Report**  
the cyberbullying  
material to the  
social media service



| 2

**Collect evidence**  
copy URLs or take  
screenshots of the material



If the content is not removed within 48 hours apply steps 3 and 4

| 3

**Report it**  
[esafety.gov.au/report](https://esafety.gov.au/report)



| 4

**Block**  
the person and  
talk to someone  
you trust



If you are in immediate danger, call **000** (triple zero)  
If you need to talk to someone, visit [kidsline.com.au](https://kidsline.com.au) or call them on  
**1800 55 1800**, 24 hours a day 7 days a week



STRIVE TO ACHIEVE

## Student ICT Agreement

The Student ICT Agreement form must be signed and returned to the school before the device is issued.

The student and parent or caregiver must carefully read this charter before signing it. Any questions should be addressed to the school and clarification obtained before the charter is signed.

In signing below, I acknowledge that I,

- accept all policies and guidelines as per the Responsible Behaviour Plan for Students
- understand my responsibilities regarding the use of the device and the internet
- acknowledge that I understand and agree with all of the conditions detailed in the Student ICT Agreement
- understand that failure to comply with the Student ICT Agreement could result in loss of access

Student's Name

Signature of Student

Date

Parent / Caregiver's Name

Signature of Parent / Caregiver

Date

Designated school representative's Name

Signature of School  
Representative

Date

**Please remove this page and return to Miles SHS  
administration office**