**Information and Communications Technology (ICT)**

**Responsible Use Procedure**

Purpose statement

* Information and communication technology (ICT), including access to and use of the internet and email, are essential tools for schools in the provision of innovative educational programs.
* Schools are constantly exploring new and innovative ways to incorporate safe and secure ICT use into the educational program.
* School students, only with the approval of the principal, may be permitted limited connection of personally-owned mobile devices to the department's network, where this benefits the student's educational program.

Authorisation and controls

* The principal reserves the right to restrict student access to the school's ICT facilities and devices if access and usage requirements are not met or are breached. However, restricted access will not disrupt the provision of the student's educational program. For example, a student with restricted school network access may be allocated a stand-alone computer to continue their educational program activities.
* The Department of Education monitors access to and use of its network. For example, email and internet monitoring will occur to identify inappropriate use, protect system security and maintain system performance in determining compliance with state and departmental policy.
* The department may conduct security audits and scans, and restrict or deny access to the department's network by any personal mobile device if there is any suspicion that the integrity of the network might be at risk.

Responsibilities for using the school's ICT facilities and devices

* Students are expected to demonstrate safe, lawful and ethical behaviour when using the school's ICT network as outlined in the [Code of School Behaviour](https://hilderroadss.eq.edu.au/SupportAndResources/FormsAndDocuments/Documents/Student%20Code%20of%20Conduct%202021-2024.pdf#search=code%20of%20school%20behaviour).
* Students are to be aware of occupational health and safety issues when using computers and other learning devices.
* Parents/guardians are also responsible for ensuring students understand the school's ICT access and usage requirements, including the acceptable and unacceptable behaviour requirements.
* Parents/guardians are responsible for appropriate internet use by students outside the school environment when using a school owned or provided mobile device.
* The school will educate students regarding cyber bullying, safe internet and email practices, and health and safety regarding the physical use of ICT devices. Students have a responsibility to behave in line with these safe practices.
* 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).
* Students cannot use another student or staff member's username or password to access the school network. This includes not browsing or accessing another person's files, home drive, email or accessing unauthorised network drives or systems. Additionally, students should not divulge personal information (e.g. name, parent's name, address, phone numbers), via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.
* Students need to understand that 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.

Responsibilities for using a personal mobile device on the department’s network

* Prior to any personally-owned mobile device being used, approval must be sought from the school to ensure it reflects the department's security requirements.
* Further information can be located in the school’s Bring-your-own-device (BYOD) Program documentation.

Sign-off

* The sign-off process for school students and their parents/guardians occurs on enrolment. It is parents’ responsibility to notify the school in writing of any changes to consent.
* **Please note:** Students from Prep to Year 3 inclusively are exempt from signing the student section below.

**HILDER ROAD STATE SCHOOL**

**ACCEPTABLE ICT USE AGREEMENT - STUDENT**

***Student****:*

* I understand that the school's information and communication technology (ICT) facilities and devices provide me with access to a range of essential learning tools, including access to the internet. I understand that the internet can connect me to useful information stored on computers around the world.
* While I have access to the school's ICT facilities and devices: I will use it only for educational purposes; I will not undertake or look for anything that is illegal, dangerous or offensive; and I will not reveal my password or allow anyone else to use my school account.
* Specifically, in relation to internet usage, should any offensive pictures or information appear on my screen I will close the window and immediately inform my teacher quietly, or tell my parents/guardians if I am at home.
* If I receive any inappropriate emails at school I will tell my teacher. If I receive any at home I will tell my parents/guardians.
* When using email or the internet I will not:
  + reveal names, home addresses or phone numbers – mine or that of any other person
  + use the school's ICT facilities and devices (including the internet) to annoy or offend anyone else.
* I understand that my online behaviours are capable of impacting on the good order and management of the school whether I am using the school's ICT facilities and devices inside or outside of school hours.
* I understand that if the school decides I have broken the rules for using its ICT facilities and devices, appropriate action may be taken as per the school's *Behaviour Management Policy*, which may include loss of access to the network (including the internet) for a period of time.
* I have read and understood this procedure/policy/statement/guideline and the [Code of School Behaviour](https://hilderroadss.eq.edu.au/SupportAndResources/FormsAndDocuments/Documents/Student%20Code%20of%20Conduct%202021-2024.pdf#search=code%20of%20school%20behaviour).
* I agree to abide by the above rules / the procedure/policy/statement/guideline.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Student's name Student’s Signature Date*

**HILDER ROAD STATE SCHOOL**

**ACCEPTABLE ICT USE AGREEMENT – PARENT / GUARDIAN**

***Parent or Guardian****:*

* I understand that the school provides my child with access to the school's information and communication technology (ICT) facilities and devices (including the internet) for valuable learning experiences. In regards to internet access, I understand that this will give my child access to information on computers from around the world; that the school cannot control what is on those computers; and that a small part of that information can be illegal, dangerous or offensive.
* I accept that, while teachers will always exercise their duty of care, protection against exposure to harmful information should depend upon responsible use by students/my child. Additionally, I will ensure that my child understands and adheres to the school's appropriate behaviour requirements and will not engage in inappropriate use of the school's ICT facilities and devices. Furthermore, I will advise the school if any inappropriate material is received by my student/child that may have come from the school or from other students.
* I understand that the school is not responsible for safeguarding information stored by my child on a departmentally-owned student computer or mobile device.
* I understand that the school may remotely access the departmentally-owned student computer or mobile device for management purposes.
* I understand that the school does not accept liability for any loss or damage suffered to personal mobile devices as a result of using the department's facilities and devices. Further, no liability will be accepted by the school in the event of loss, theft or damage to any device unless it can be established that the loss, theft or damage resulted from the school's/department's negligence.
* I believe \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ *(name of student)* understands this responsibility, and I hereby give my permission for him/her to access and use the school's ICT facilities and devices (including the internet) under the school rules. I understand where inappropriate online behaviours negatively affect the good order and management of the school, the school may commence disciplinary actions in line with this user agreement or the *Behaviour Management Policy*. This may include loss of access and usage of the school's ICT facilities and devices for some time.
* I have read and understood this procedure/policy/statement/guideline and the [Code of School Behaviour](https://hilderroadss.eq.edu.au/SupportAndResources/FormsAndDocuments/Documents/Student%20Code%20of%20Conduct%202021-2024.pdf#search=code%20of%20school%20behaviour).
* I agree to abide by the above rules / the procedure/policy/statement/guideline.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Parent's name Parent’s Signature Date*

The Department of Education through its Information privacy and right to information procedure is collecting your personal information in accordance with the [*Education (General Provisions) Act 2006* (Qld)](https://www.legislation.qld.gov.au/view/html/inforce/current/act-2006-039) in order to ensure:

* appropriate usage of the school network
* appropriate usage of personal mobile devices within the school network.
* The information will only be accessed by authorised school employees to ensure compliance with its [Information privacy and right to information procedure](http://ppr.det.qld.gov.au/corp/ict/management/Pages/Information-Privacy-and-Right-to-Information.aspx). Personal information collected on this form may also be disclosed to third parties where authorised or required by law. Your information will be stored securely. If you wish to access or correct any of the personal information on this form or discuss how it has been dealt with, please contact your child's school. If you have a concern or complaint about the way your personal information has been collected, used, stored or disclosed, please also contact your child's school.

**CYBERSAFETY IN QLD SCHOOLS**

Cybersafety refers to online behaviour that is safe, appropriate and responsible.

To help prevent cybersafety incidents, students are taught how to:

* use technology appropriately and responsibly
* behave in ways to enhance their own safety.

**Information for Students**

Everything that you share, like, comment and post online contributes to your digital identity. Your audience can be bigger than you realise.

When you are online never give away your home address, phone number, email address and passwords or any other personal information.

If you don’t know and trust someone in the real world, delete or block them online. Don’t be fooled by fake profiles or mutual friend suggestions.

Make positive choices. Stay in control of your online world. If you make poor choices while on social media or online games there may be social or legal consequences.

When you are online never give away your home address, phone number, email address and passwords. You should treat strangers the same way online as you would in the real world.

**Information for Parents**

Remember, you already possess the skills to supervise. Apply these skills to technology and the online world.

To help keep your child safe when they are online, you can:

* put computers in open spaces within your home
* remind your child that content can be posted instantaneously, the downfall is that they can potentially post something without thinking about the ramifications.
* educate your child about appropriate online behaviour and the need for respectful communication with other internet users
* keep an eye on what your child is doing online (both in the home and on any mobile devices they may have access to e.g. phones, music devices and tablets)
* set clear rules about what sites and activities they are allowed to access
* install software to limit their use and monitor/restrict the sites they visit
* discuss a plan with your child about how to address any cybersafety issues that may arise (make sure they know you will be supportive if they mention anything and that they will not get in trouble)
* encourage them to find someone they feel safe talking to, such as yourself, a relative, a teacher or a trusted adult.