St Joseph’s Catholic Primary School, Tweed Heads

Digital Devices Acceptable Use Policy 2015
(incorporating BYOD)

Digital Technologies and Devices Policy and Procedures
**Rationale**

As Catholic educators our primary goal is to educate the students in our care and to ensure they are kept safe and protected, particularly while engaging with learning technologies in contemporary learning environments. At St Joseph’s we acknowledge and value the role technology plays in supporting learning and teaching and strive to embed appropriate technologies within contemporary pedagogies. We will provide educational opportunities which build on and extend the ways in which they learn and communicate, supporting new approaches to learning centred around creativity and innovation, critical thinking, problem solving, decision making, collaboration and communication and life-long learning. The school policy is to encourage student use of devices as an integral part of their learning.

As a primary school community striving to serve the needs of our young people in an authentic way, this *Digital Technologies and Devices Policy* gives practical expression to our school’s key learning and teaching principles. One of the key ways to do this is through integration of technology to ensure that all students have the opportunity to become competent, discriminating and creative users of a range of technologies. Such integration of technologies has the potential to engage students in ways not previously possible, to enhance their achievement, to create new learning possibilities and to extend students’ interaction with their local and global communities. The integration of technology also facilitates the relational nature of learning, providing new opportunities for parents to engage with teachers, learning programs and their child’s progress.

While providing the opportunity to enhance and extend human interaction, empathy and understanding, the misuse of information and communication technologies can significantly damage an individual’s dignity. Significantly, this policy calls attention to an individual’s right to freedom from harassment, humiliation and bullying.

I encourage a close reading of this Policy and the Agreements by parents and students and acknowledge the work of our staff, along with various personnel from the Catholic Schools Office (CSO), in drafting this Policy. The launch of this Policy is a significant step in our commitment to build learning strategies which realise our overarching vision at St Joseph’s.

**School Context**

This *Policy and Agreement* addresses student use of school and personal devices (Bring Your Own Devices BYOD) within St Joseph’s Primary School, Tweed Heads. It also includes access to and usage of Devices, Services (including the Internet) and Digital Technologies including but not limited to:

- Email and instant messaging
- Social networking sites (eg. Instagram)
- Video and photo sharing websites (eg. Picassa, Youtube)
- Corporate and personal blogs
- Micro-blogs (eg. Twitter)
- Forums and discussion groups (eg. Moodle)
- Wikis
- Vod and Podcasts,

The Policy and Agreements are designed to ensure that staff, parents and students understand the rules that apply to technology use within the school context. The same standards of good and appropriate behaviour that are expected in our staffroom, playground and classrooms are expected when using the school and personal Devices, Technologies and Services.
The students of St Joseph’s are provided with the Google Apps for Education suite of products for use in curriculum related activities and for collaboration and communication with the teacher and other students. Their account includes access to an email account (Google mail), Google drive, calendar, sites, and documents. These applications are accessible both from school and the home if an internet connection is available. Students are also able to access a variety of other services including printing and internet access while on site. This internet access is filtered by the Catholic Schools Office, Lismore. This filter, as far as possible, restricts St Joseph’s users access to sites which have been deemed inappropriate. e.g all social media sites. This filter is not active in the home environment, and therefore parents are asked to supervise student Internet access at home.

The cost of providing network infrastructure, upgrades, training, licensing, servicing, Internet access, filtering, school based applications and cloud storage is met by the school.

Users of the St Joseph’s system are not to store, play or share information on the network or on any device that is inappropriate. Inappropriate material is defined as including, but not limited to:

- Illegal or unlicensed software, video and music files that contravene copyright, and content rated above ‘G’.
- Unacceptable remarks, including offensive, abusive or discriminatory comments.
- Threatening, bullying or harassing material or demands including images, video, audio and text.
- Explicit or suggestive material or correspondence including images, video, audio and text.
- False or defamatory information about a person or organisation including images, video, audio and text.
- Using the school name or crest without the written permission of the Principal

If users are found to have accessed, stored or shared inappropriate material on devices or the network they will be in breach of this policy and subject to the school Discipline Policy and associated Behaviour Management Plan.

The Catholic Schools Office advocates the use of the Cyber Safety Help button created by Cybersmart. Cybersmart is a national cybersafety and cybersecurity education program managed by the Australian Communications and Media Authority (ACMA), as part of the Australian Government’s commitment to cybersafety. Students are supported through the explicit teaching of Digital Citizenship and responsible use of technology from Kindergarten to Year 6 through age appropriate educational resources and stage-based content in Digital Citizenship which includes Cyberbullying.

St Joseph’s School has an Anti-Bullying Policy (including Cyber Bullying) that clearly states the expected standards of student behaviour. These standards should be read in conjunction with this policy.

The school will investigate and take action where ethical, safety and security issues, behaviours and concerns arise in school and outside of school when it causes significant harm to the relationships between students and or teachers, or is criminal in nature or has the capacity to impact on relationships across the wider school community.

1. When using school and personal devices and services students will:
   - Ensure that they access the Internet only within the school proxy and filtering system provided.
   - Sim cards are to be removed by students from any device prior to entry into the school. If students have accidentally brought a Sim card enabled or alternate tether enabled device, teachers must confiscate the Sim card or tethering device for the duration of the school day and make contact with parents/carers.
   - Ensure that communication through Internet and email services is related to learning.
   - Log off at the end of each session to ensure that nobody else can use their account.
   - Promptly tell their teacher if they suspect they have received a computer virus or spam (i.e. unsolicited email) or if they receive a message that is inappropriate or makes them feel uncomfortable or unsafe.
   - Seek advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student.
   - Use appropriate privacy controls for all internet and app based activities. e.g. turning off geo location settings
- Ensure that school services are not used for unauthorised commercial activities, buying and/or selling items online, online gambling or any unlawful purpose.

2. When using the school services or personal mobile phones (or similar personal equipment) students will not, and will not attempt to:
   - Disable settings for virus protection, spam and internet filtering that have been applied by the school and not attempt to evade them through use of proxy sites.
   - Access, post or send inappropriate internet or email content, especially content that is illegal, dangerous, obscene or offensive
   - Allow others to use their personal accounts.
   - Deliberately use the digital identity of another person to send messages to others or for any other purposes.
   - Enter ‘chat’ or ‘social networking’ internet sites without the permission of a teacher.
   - Intentionally download unauthorised software, graphics or music that are not associated with the learning activity as directed by a staff member.
   - Damage or disable computers, computer systems or networks or distribute damaging files or viruses.
   - Trespass in another person's folders, work or files.
   - Disclose personal information about another person (including name, address, photos, phone numbers)
   - Distribute or use information which is copyrighted without proper permission.
   - Capture, record, store, transfer or upload audio, images, video or text of any members of the school community without their consent and under direct instruction from the teacher for educational purposes only.
   - Keep personal information, including names, addresses, phone numbers, photographs, credit card details, iTunes account logins and telephone numbers, of themselves or others, private.
   - Use inappropriate or obscene language that may be offensive to other users
   - Make personal attacks on or about other people
   - Send, post or upload false information about a person, group or organisation that might injure the reputation of that person, group or organisation

Students who do not own a digital device may use a school-owned device, which remains the property of St Joseph’s and is subject to the same policy and user agreements as a BYOD.

**Access and Use of Services and Facilities**

In order to be compliant within the Diocese of Lismore Catholic Schools Office, provide secure access to a range of services and enforce security restrictions and compliance policies when devices are connected to the school network St Joseph’s school will use the Airwatch Mobile Device Management tool.

To join the school network and take advantage of the services and resources available, students will need to have the application (Airwatch MDM Agent) installed on their personal device. This application is free to download from the Google Play or Apple Store and must be installed prior to the use of the device on the school network. This application allows the user to connect to the school network which provides free filtered access to internet sites. This application also allows the school to resource the student device with school purchased applications for student use at school. These applications include an internet browser (chrome), the Google Apps for Education suite and an application to allow printing to the school printers.

The school will notify parents when Apps have been purchased and made available to students at no cost. Parents must ensure the student device has the Airwatch application installed and consents to its use to allow student access to school services and resources, including the Internet. St Joseph’s school reserves the right to hold device information and track devices connected on the school network using the Airwatch App. The use of the Airwatch MDM Application will not in any way interfere with the functionality of the device when used at home or outside the school environment.
Regulations and Conditions of Use of BYOD (Bring your own Devices)

Devices:
Once the user agreement is signed by the parent and student, students are then able to bring to school and use an Apple i-Pad, which is appropriately protected in an approved case. This device must also support the installation of particular applications which staff will ask students to use in class. Each parent and student needs to accept responsibility for the care and maintenance of their own device.

Battery Charging:
Student owned Devices are to be charged at home. Students are required to bring their device to school each day fully charged.

Applications:
All students will have filtered access Internet and access to the Google suite of Applications and are solely responsible at all times for their proper use. Additional applications will be required in the future and parents will be informed of what they are so they can install them. A list of required applications will be provided to parents for their child’s Device. These applications must be on the Device at all times. Students may install additional applications if relevant to learning experiences and they are age appropriate. In a primary school this means that all content must be rated ‘G’ unless the teacher requires it and permission is given by parents. The school may also provide applications to students at no cost via the Airwatch application.

Acceptable Use:
Devices are to be brought to school every day. Teachers will inform students on any days that the Device will not be required such as swimming carnivals and other special event days. Students are only permitted to use their Devices at school during supervised learning time. They are not permitted on the playground at any time.

Students must be aware of and abide by the Student User Agreement. Any breach of this is considered serious and disciplinary action will be taken.

If a student is found to be using a device or associated technology, such as the camera, inappropriately or accessing or sharing inappropriate material, the device will be confiscated and may result in restricted use, loss of privileges, disciplinary action and parents contacted. In some circumstances the involvement of appropriate authorities such as the Police may be required. All images, videos and recorded files must be immediately deleted after use or as directed by the teacher.
**POLICY DATES**

<table>
<thead>
<tr>
<th>POLICY DATES</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Formulated</td>
<td>19/12/2014</td>
<td>Adopted</td>
</tr>
<tr>
<td>Implemented</td>
<td>01/02/2015</td>
<td>Reviewed</td>
</tr>
<tr>
<td>Next Review Due</td>
<td>19/12/2015</td>
<td></td>
</tr>
</tbody>
</table>

**POLICY AUTHORISATION**

<table>
<thead>
<tr>
<th>Principal</th>
<th>Mr Tony Boyle</th>
<th>Signature</th>
</tr>
</thead>
</table>