

# Computer Facilities and External Networks (ICT) Acceptable Use Policy

---

## Related Policies

Bullying Policy  
BYOD (iPads) Care and Use Policy, including *iPad Student User Agreement*  
Child Protection Policy (ACT)  
Code of Conduct Policy  
Communication Policy  
Mobile Phone and Electronic Devices Policy  
Privacy Policy  
Student Welfare and Management Policy  
Catholic Education - IC and LT Policies

**This policy is based on Archdiocese of Canberra and Goulburn Catholic Education Office Computer Facilities and External Networks (ICT) Acceptable Use policies and the associated CE Service Level Agreement.**

## Purpose

This policy outlines how all parties involved can work together to embrace the educational potential of Information Communication Technologies (ICT) within a safe and supportive environment.

## Policy

At St Thomas the Apostle Primary School we provide student and staff access to ICT based on the following principles:

- Access to and content of technology use must always be referenced to curriculum and developmental educational needs of the students.
- Developing skills in the use of ICT is an important life lesson and can be used to engage and inspire students to fulfil learning potential in all curriculum areas.
- Staff have a duty of care to ensure students are safe in online environments and are taught the skills to avoid unsafe situations.
- Information created, produced, communicated, stored or accessed on school ICT are subject to monitoring by the school or CE.
- Acceptable Use Agreements for students and staff must be read and signed at the beginning of each year. Parents are asked to co-sign student agreements. These agreements outline rights and responsibilities of staff and students. These documents are attached to this policy.
- Parents are informed that this policy is available from the school or on the school website and are encouraged to assist staff in facilitating appropriate use of ICT.
- Staff and students (and their parents) are to keep passwords private.

## Definitions

**Information and Communication Technology (ICT)** refers to:

a) Computer hardware and associated equipment. This covers, but is not limited to, computers, cameras, iPads, mobile phones, printing and access to the school/CE network.

- b) Computer software and web-based activities including email, apps, social media sites and internet use.
- c) All telecommunications devices and facilities that are owned by the school or personal devices that are connected to the school's network.

**External Networks** refers to online environments and facilities, including the World Wide Web (www), cloud storage and online learning platforms.

**Acceptable Use** includes those lawful uses that are related to the core business of the school and includes incidental personal use of devices and networks. Incidental personal use is defined as use by individual staff or students for occasional personal communication or information, as long as such use does not interfere with school operations, other users, is lawful and complies with this policy.

**Teaching and Learning Specialist (TLS)** is the school appointed staff member that supports staff in the use of ICT in the classroom.

**CE or CEO** refers to the office of Catholic Education Archdiocese of Canberra & Goulburn

## **Procedures**

### **Access to ICT**

All staff and students are provided with a log-on to the school network, the CE network including internet access, email and learning platforms. An individual log-on consists of a username and password supplied by the school. Students and staff can use their school log-on from computers outside of the school environment to access web-based sites and platforms subscribed to by the school. Users are reminded of the extreme importance of not sharing their passwords under any circumstances. All year levels undertake cyber safety activities within the first few weeks of the new school year. These activities are revised through the year to ensure the safety of the students.

### **Security and Safety Measures**

- Filtering software is in place to prevent access to inappropriate web sites. The Teaching and Learning Specialist (TLS) can organise for there to be security settings for individual web addresses, words and images.
- No filtering is fail-proof, so students are taught the steps to take if they come across unsuitable content. Automated reports of searches breaching the security rules are sent to the nominated school executive/administrator.
- Emails are filtered. Unacceptable language and content is redirected to the nominated school executive/administrator. Content and usage of emails and other electronic communications may be monitored. This includes communications sent from home using school provided services.
- All messages and files stored on school and CE systems, and shared online platforms will be treated as education related and may be monitored. Accordingly students should not expect that any message or file transmitted or stored on school computer facilities and external networks will be private.
- Students are expected to let teachers know of bullying or inappropriate content in emails or messages they receive or unacceptable websites they find. These will then be dealt with following the Student Welfare and Management Policy of the school.
- Children and teachers are encouraged to check school owned equipment before use and ensure it is returned in the same condition.
- Teachers are to report damages to the TLS.

- Mobile phones and electronic devices are to be kept with the classroom teacher as per the Mobile Phone and Electronic Devices Policy.
- The protective behaviours encouraged in the school are:
  1. If you see something inappropriate on your computer screen then turn the monitor off immediately.
  2. Notify an adult who will take care of it for you.
  3. Adult notifies the TLS to deal with the incident, which may involve filtering that URL.
- If parents discover inappropriate content on their child's device at home they are to deal with the situation accordingly. If this content relates to a school context parents are recommended to inform the school.

### **Use of Personal Devices**

- Use of personal devices brought to the school will be governed by this policy and the Acceptable BYOD (iPads) Care and Use Policy and Mobile Phone and Electronic Devices Policy.
- Technical support will be provided by CE Information Communication & Learning Technology Services to schools in accordance with the Service Level Agreement.
- Devices owned by students may be searched and/or confiscated if the principal believes, on reasonable grounds, that there is a threat to a person or system security or the device has been used or involved with unlawful conduct or a serious breach of the Acceptable Use Agreement.
- Whilst using personal electronic devices at school, students must access the Internet through the school wireless network.

### **Acceptable Use Guidelines**

#### **School Responsibilities:**

- Provide and maintain a suitable level of ICT.
- Liaise with the CE ICT service team and ICT curriculum team.
- Implement the CE's Computer Facilities and External Networks – Acceptable Use by Students Policy.
- Provide opportunities for the development of ICT that provides the students with the skills that they need to be able to embrace technology in today's world and into the future.
- Offer a curriculum that integrates the use of ICT and provides opportunities for students to build skills in using current technology.
- In conjunction with the CE, provide a monitoring, filtering and virus protection service for internet use.
- The School Leadership Team and TLS will monitor use of the school ICT, ensuring students' rights to privacy and personal wellbeing are maintained.
- Offer all staff the opportunity to participate in professional development to gain the most potential from using and teaching with ICT.
- Stay informed of legal issues associated with using ICT in education.
- Maintain the school website.
- Ensure that information published on the internet by the students or school under the school's name, meets legal requirements and standards of general practice within the community in relation to copyright and safety.
- Provide access and information regarding the Acceptable Use Policy to each family.
- Distribute and collect signed Computer Facilities and External Networks – Acceptable Use by Students Agreements (see Appendix 1).
- Distribute and collect Computer Facilities and External Networks - Acceptable Use by Staff Agreement <https://intranet.cg.catholic.edu.au/StaffServices/Policies/>
- Issue new users with log-on names and passwords.

### **Teacher Responsibilities:**

- Always supervise student use of ICT, in particular internet-based use. The teacher should be roaming the room to ensure all students are using ICT appropriately. This duty of care extends beyond class use to all student use in shared spaces such as library and break-out areas.
- Teach students how to use the internet safely, how to analyse and evaluate the information they find and to know about copyright laws. Each year all students will be made aware of websites encouraging the use of safe internet practices.
- Discuss with students the concept of digital citizenship and issues of cyber bullying and online privacy.
- Integrate the use of ICT across the curriculum.
- Monitor and teach responsible use of all hardware devices, printers, web-based and software applications.
- Distribute and collect signed Computer Facilities and External Networks (ICT) - Student Acceptable Use Agreements before the student is allowed to use ICT each year.
- Read and sign Computer Facilities and External Networks Agreement - Acceptable Use by System Staff.

### **Student Responsibilities:**

- Discuss the Computer Facilities and External Networks (ICT) - Student Acceptable Use Agreements with parents and teachers.
- Follow the conditions set out in the Computer Facilities and External Networks (ICT) - Student Acceptable Use Agreement and Year 5/6 Student iPad User Agreement.
- Use class or individual log-on details to gain access to facilities or networks.
- Keep their username and password private from other students. Share their details with parents as required.
- Develop skills in using ICT to conduct research, communicate with others, publish and submit work and extend learning in curriculum areas.
- Limit the use of printing and downloading in consideration of the costs involved in providing these facilities.
- Use school ICT facilities for educational purposes and in a way that complies with this policy and does not interfere with other people's use of the facilities.
- Immediately report any breach of security or privacy; inappropriate download, offensive material, virus or cyber-bullying to a responsible adult.

### **Parent Responsibilities:**

- Speak to their child's teacher, the TLS or school principal if they have any questions or concerns regarding use of the school's ICT.
- Read with their child and sign the Computer Facilities and External Networks (ICT) - Student Acceptable Use Agreement (see Appendix 1).
- Discuss privacy, safety and cyber-bullying issues with their child.
- Help their child to keep the copyright laws.
- Monitor their child's use of ICT at home.
- Discuss with their child how they use ICT at school.

### **References**

St Thomas the Apostle Core Curriculum Document  
Every Chance to Learn (ACT)

Australian Curriculum General Capabilities and the Digital Technologies Curriculum (Draft)  
Cyber safety - [www.cybersafety.dbcde.gov.au](http://www.cybersafety.dbcde.gov.au)

<https://intranet.cg.catholic.edu.au/StaffServices/Policies/> Policies for staff and student use.

## **Forms**

### **Appendix 1**

St Thomas the Apostle Catholic Primary School Computer Facilities and External Networks (ICT) - Student Acceptable Use Agreement

### **Appendix 2 - Found on CE website**

Archdiocese of Canberra and Goulburn Catholic Education Office

Computer Facilities and External Networks Agreement – Acceptable Use by System Staff

<https://intranet.cg.catholic.edu.au/StaffServices/Policies/>

### **Appendix 3**

Archdiocese of Canberra and Goulburn Catholic Education Office

Workplace Surveillance Notice

**Approved by:** Principal

**Issuing Group:** St. Thomas the Apostle Primary School

**Implementation Date:** 2016

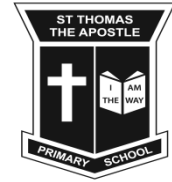
**Supersedes Policy Dated:** 2013

**Policy Last Updated:** September 2015

**Review Date:** 2016

## Appendix 1

### **St Thomas the Apostle Catholic Primary School Computer Facilities and External Networks (ICT) Student Acceptable Use Agreement 2015**



To have access to Information and Communication Technologies (ICT) at St Thomas the Apostle you need to follow these agreed practices.

#### **Student Agreement**

Using ICT at school is a privilege. I have conditions to follow, which are for the safety and privacy of myself and others.

I will:

- Treat the school's ICT equipment with care and use it responsibly for educational purposes.
- Use devices and internet the way my teacher(s) has asked me to.
- I will turn off the monitor, then tell my teacher or another adult immediately if I find something that is not appropriate for school children on the internet or school network.
- Publish work, send emails and post messages using language I know is acceptable in my school.
- Tell the teacher if I receive a message that makes me feel uncomfortable.
- Respect the privacy of all computer users at school by correctly using passwords and opening only my own work and emails.
- Pack away equipment and tidy the area I was using.

I will not:

- Give out personal information that could be used to identify me, my family or friends, such as surname, address, phone number or photo while using the internet.
- Pretend to be another person when communicating on the internet.
- Break copyright law by copying and/or using another's work.
- Write or send messages that would make another person feel uncomfortable.
- Pass on information about inappropriate material or sites to other students.
- Misuse the internet or encourage others to do so.
- Waste materials through excessive printing and downloading.
- Download any software or files, store files, install software, or change computer or other device settings without the permission of a teacher.
- Access social media on any device at school, without explicit teacher direction.
- Post any images, videos or comments about any member of my school community or myself that might give my school a bad name and offend a member of the school community.
- Upload images of other members of the school without their permission.
- Upload any images of myself or other students in uniform or identified with the school in any other way without the permission of the principal.
- Bring personal devices to school and use them on the playground.

Student's signature (Year 3 and above) \_\_\_\_\_

Name (print) \_\_\_\_\_ date: \_\_\_\_\_

#### **Breaking the Student Agreement**

If a student breaks the Student Agreement a number of steps can be taken:

- Appropriate ICT rights withdrawn.
- Withdrawal of individual log-on to intranet, internet or both for a period of time as deemed appropriate.
- Parents notified.
- Guidance from the Learning Technologies Specialist or School Executive as to how to avoid future problems.
- Steps as outlined in the School's *Student Welfare and Management Policy*.

***PTO for Parent Acknowledgement***

## Parent Acknowledgement

I  give /  do not give (circle one) permission for my son/daughter  
\_\_\_\_\_ (name) in \_\_\_\_\_ (class) to use the internet and other ICT facilities.

- I have read the *Computer Facilities and External Networks (ICT) Acceptable Use Policy*, containing acceptable use guidelines and the *Student Acceptable Use Agreement*. A copy can be viewed on the school website at [www.sttap.act.edu.au](http://www.sttap.act.edu.au)
- I agree to my child using Information and Communication Technologies for educational purposes in the manner outlined in the policy.
- I agree to my child transmitting work electronically to teachers and having the work published where the school considers to be appropriate.
- I have talked to my child about safety, privacy and copyright concerns when using computers at school and home.
- I consent to my child's use of the school's student email system on the understanding that the system is provided through Google Apps for Education and that, consequently, students' emails and email account details may be transferred, stored and processed in the United States or other country utilised by Google to provide the Google Apps services. Information about the security and privacy features of Google Apps for Education may be found at <https://www.google.com/enterprise/apps/education/benefits.html>

Parent/Guardian's signature: \_\_\_\_\_

Name (print): \_\_\_\_\_ Date: \_\_\_\_\_

**Please return this form to school as soon as possible.**

**Your child will be unable to use the school's ICT facilities, including internet, until this form is returned. Thank you.**

## Appendix 3



Archdiocese of Canberra and Goulburn  
CATHOLIC EDUCATION OFFICE

### **WORKPLACE SURVEILLANCE NOTICE (NSW)**

All messages on the CE's system will be treated as business or education related messages which may be monitored. Accordingly you should not expect that any information or document transmitted or stored on the CE's computer facilities and external networks will be private.

From time to time the content and usage of email may be examined by the CE or the School Principal or a third party on the CE's behalf. This will include electronic communications which are sent to you or by you, both internally and externally.

You should also be aware that the CE is able to monitor your use of the internet, both during working hours and outside of those hours. This includes the internet sites and content that you access and the length of time you spend using the internet.

CE monitoring of its computer facilities and external networks is ongoing and is consistent with the *Workplace Surveillance Act 2005* (NSW).

### **WORKPLACE SURVEILLANCE NOTICE (ACT)**

All messages on the CE's system will be treated as business or education related messages which may be monitored. Accordingly you should not expect that any information or document transmitted or stored on the CE's computer facilities and external network will be private.

From time to time the content and usage of email may be examined by the Principal or the CE or by a third party on the CE's behalf. This will include electronic communications which are sent to you or by you, both internally and externally.

You should also be aware that the CE is able to monitor your use of the internet, both during working hours and outside of those hours. This includes the internet sites and content that you access and the length of time you spend using the internet.

CE monitoring of its Computer Facilities and External Networks is ongoing and is consistent with the *Workplace Privacy Act 2011* (ACT).