Katandra School, Ormond	**DIGITAL TECHNOLOGIES POLICY (INTERNET, SOCIAL MEDIA & DIGITAL DEVICES)**	Katandra School — Providing the best learning environment for your child

PURPOSE

To ensure that all students and members of our school community understand:

- our commitment to providing students with the opportunity to benefit from digital technologies to support and enhance learning and development at school including our 1-to-1 personal device program;
- expected student behaviour when using digital technologies including the internet, social media, and digital devices (including computers, laptops, tablets);
- the school's commitment to promoting safe, responsible and discerning use of digital technologies, and educating students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and digital technologies; and
- our school's policies and procedures for responding to inappropriate student behaviour on digital technologies and the internet.

SCOPE

This policy applies to all students at Katandra School.

Staff use of technology is governed by the Department's *Acceptable Use Policy.*

DEFINITIONS

For the purpose of this policy, "digital technologies" are defined as being any networks, systems, software or hardware including electronic devices and applications which allow a user to access, receive, view, record, store, communicate, copy or send any information such as text, images, audio, or video.

POLICY

(a) Vision for Digital Technology at Our School

Katandra School understands that digital technologies including the internet, apps, computers and tablets provide students with rich opportunities to support learning and development in a range of ways.

Through increased access to digital technologies, students can benefit from enhanced learning that is interactive, collaborative, personalised and engaging. Digital technologies enable our students to interact with and create high quality content, resources and tools. It also enables personalised learning tailored to students' particular needs and interests and transforms assessment, reporting and feedback, driving new forms of collaboration and communication.

Katandra School believes that the use of digital technologies at school allows the development of valuable skills and knowledge and prepares students to thrive in our globalised and inter-connected world. Our school's vision is to empower students to use digital technologies to reach their personal best and fully equip them to contribute positively to society as happy, healthy young people.

User agreements for Digital technologies at Katandra School are distributed annually, a copy can be seen in Appendix 1 at the end of the document.

(b) iPads at Katandra School

Classes at Katandra School are delivered with the use of iPads. Students are provided with a 1:1 iPad at school each day to be used during class time for different learning activities. Within the parent payment levy there is a cost associated to the ongoing cost and purchase of Apps to support the students learning.

If a student or staff member brings their own iPad to school it should be noted: that our school does not have insurance to cover accidental damage to students' or staff iPads, and parents/carers are encouraged to consider obtaining their own insurance for their child's iPad.

(c) Safe and Appropriate Use of Digital Technologies

Digital technology, if not used appropriately, may present risks to users' safety or wellbeing. At Katandra School, we are committed to educating all students to be safe, responsible and discerning in the use of digital technologies, equipping them with skills and knowledge to navigate the digital age.

At Katandra School, we:

- use online sites and digital tools that support students' learning, and focus our use of digital technologies on being learning-centred;
- restrict the use of digital technologies in the classroom to specific uses with targeted educational or developmental aims;
- supervise and support students using digital technologies in the classroom;
- effectively and responsively address any issues or incidents that have the potential to impact on the wellbeing of our students;
- have programs in place to educate our students to be promoting safe, responsible and discerning use of digital technologies, including [insert details of specific programs];
- educate our students about digital issues such as online privacy, intellectual property and copyright, and the importance of maintaining their own privacy online;
- actively educate and remind students of our *Student Engagement* policy that outlines our School's values and expected student behaviour, including online behaviours;
- have an Acceptable Use Agreement outlining the expectations of students when using digital technology at school;
- use clear protocols and procedures to protect students working in online spaces, which includes reviewing the safety and appropriateness of online tools and communities, removing offensive content at earliest opportunity;
- educate our students on appropriate responses to any dangers or threats to wellbeing that they may encounter when using the internet and other digital technologies;
- provide a filtered internet service to block access to inappropriate content;
- refer suspected illegal online acts to the relevant law enforcement authority for investigation; and

- support parents and carers to understand safe and responsible use of digital technologies and the strategies that can be implemented at home through regular updates in our newsletter and annual information sheets.

Distribution of school owned devices to students and personal student use of digital technologies at school will only be permitted where students and their parents/carers have completed a signed Acceptable Use Agreement.

It is the responsibility of all students to protect their own password and not divulge it to another person. If a student or staff member knows or suspects an account has been used by another person, the account holder must notify the classroom teacher and digital technologies coordinator as appropriate, immediately.

All messages created, sent or retrieved on the school's network are the property of the school. The school reserves the right to access and monitor all messages and files on the computer system, as necessary and appropriate. Communications including text and images may be required to be disclosed to law enforcement and other third parties without the consent of the sender.

(d) Student Behavioural Expectations

When using digital technologies, students are expected to behave in a way that is consistent with Katandra School's *Statement of Values, Student Wellbeing and Engagement* policy, and *Bullying Prevention* policy.

When a student acts in breach of the behaviour standards of our school community (including cyberbullying, using digital technologies to harass, threaten or intimidate, or viewing/posting/sharing of inappropriate or unlawful content), Katandra School will institute a staged response, consistent with our policies and the Department's *Student Engagement and Inclusion Guidelines.*

Breaches of this policy by students can result in a number of consequences which will depend on the severity of the breach and the context of the situation. This includes:

- removal of network access privileges;
- removal of email privileges;
- removal of internet access privileges;
- removal of printing privileges; and
- other consequences as outlined in the school's *Student Wellbeing and Engagement* and *Bullying Prevention* policies.

REVIEW CYCLE

This Code of Conduct or Policy was endorsed/approved by the Katandra School Council on November 2018 for review if legislative or other changes require in the interim or no later than November 2022.

Date Implemented	November 2018
Author	Rhett Watts
Approved By	School Council
Approval Authority (Signature & Date)	School Council President: Mario Delosa Signature: Date:
Date Reviewed	November 2022
Responsible for Review	Rhett Watts, Wendy Sheppard, Jacqui Lamden
References	Victorian Government Schools Reference Guide

APPENDIX 1-

Katandra School
Information Communications Networks
Student User Agreement

Terms of Use Agreement

1. Access to the Katandra Network

Subject to complying with this policy, all students have the right to equal access to network resources. No student is to deliberately congest the network with heavy traffic for non-academic purposes.

2. Monitoring

The Schools reserves the right to review and remove any material on user-accounts or file-share space in order to determine the appropriateness of specific uses of the network. In reviewing and monitoring user-accounts and file-share space, the Schools shall respect the privacy of user-accounts. Please note that any email containing offensive language is automatically redirected to the system administrator's desktop.

If at any time there is a reasonable belief that Katandra ICT resources are being used in breach of this Policy, the principal or line manager of the person who is suspected of using Katandra ICT resources inappropriately may suspend a person's use of Katandra ICT resources and may require that the equipment being used by the person be secured by the principal or line manager while the suspected breach is being investigated.

3. Security

Do not attempt, nor assist others, to gain access to the system in an unauthorised way, or in any way that threatens its secure operations. The user also agrees to have an up to date anti-virus program installed on their device before connected to the Katandra Network.

4. Copyright

Attempts to copy licensed, patented or copyright software provided for your use is prohibited. Students must not install their own software on the Schools systems.

5. Ownership

Students and Staff that choose to bring their own device from home agree that in the event of loss, theft or damage, Katandra is in no way responsible. It is up to the owner of the device to ensure adequate insurance has been acquired for use on this network, and that limited support from On-Site technicians is available for wireless access only.

6. Vandalism

Acts of vandalism are strictly prohibited. This includes, but is not limited to:

- The creation or uploading including but not limited to: virus, spyware, malware, which is strictly forbidden.
- Attempting to damage any networks, software or any equipment or system forming part of the network.
- Interfering with the data of other users on the network.
- Intentional physical damage.

7. Harassment

Harassment is defined as the persistent annoyance of another user, or interference with another user's work. Harassment includes, but is not limited to:

- The sending of unwanted mail.
- Posting anonymous messages.
- Hiding or altering facilities or files.

8. Improper Use of Telecommunication Services

A person shall not knowingly or recklessly:

- Use a telecommunication service supplied by a carrier to menace or harass another person.
- Use a telecommunication service supplied by a carrier in such a way as would be regarded by reasonable persons as being, in all circumstances, offensive. (An abstract from Section 85ZE of the Commonwealth Crimes Act).

9. Privacy

Students must respect the School's rights relating to privacy, the confidentiality of other network users and comply with the laws relating to privacy. Thus, students are prohibited from:

- Providing personal information about another student.
- Attempting to guess passwords or gaining unauthorised access to another person's files or reading their communications.
- Sending personal information such as your home address or telephone number through the Internet. The School's address is acceptable, but not the School's phone number.

- Disclosing your own or another person's password.

10. Defamation

Katandra ICT resources must not be used to send material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or DEECD liability. Electronic communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and widespread.

11. Unacceptable Uses of the ICT Network and the Internet

- Using the network for purposes relating to 'chain letters', or broadcasting to lists of individuals in such a manner that might cause congestion of the network.
- Downloading, storing, creating, sending or printing files or messages that are deemed to be profane, obscene, or that use language that offends or tends to degrade others.
- Giving personal information or agreeing to meet any person contacted through the Internet.
- Accessing offensive, dangerous or potentially destructive information.
- Engaging in commercial activities is not acceptable. Using the network for product advertisement or political lobbying is also prohibited. The facilities must not be used to defraud or to create false or misleading information.
- Transmitting material in violation of any government regulation is prohibited. This includes, but is not limited to, material under copyright, threatening or obscene material, or material protected by trade secret.
- Providing electronic copy (or hard copy) of your work to other students to gain or confer an unfair advantage is prohibited.
- Disadvantaging other network users by monopolising equipment or wasting computer resources is not acceptable. This includes but is not limited to:
  - o Printing unnecessarily.
  - o Spending unnecessary time on the Internet.
  - o Watching unnecessary videos on live streaming or YouTube.
  - o Sharing personal files and folders.
  - o Downloading and/or installing any software including games, chat programs etc

I _____ Hereby accept the following terms and conditions of the Katandra ICT Policy, and understand that any violations may result in any networked accounts or features of the Katandra infrastructure maybe terminated. And any necessary actions including law enforcement may be taken if needed.

Student Signature: _____

Parent / Guardian: _____