Department of Primary Industries

Tocal College

January 2024

Tocal College Internet and Social Media Policy

SECTION A Introduction

This Internet and Social Media Policy applies to:

- the use of the Department of Primary Industries (Tocal) network and all ICT equipment & devices whether on or offsite.
- all privately owned ICT equipment & devices that access the Tocal network.
- the use of privately owned ICTs when related to Tocal or the Tocal community.

The overall goal of this policy is to create and maintain a cybersafety culture that is in keeping with the values of the College and legislative and professional obligations.

This policy includes information about the obligations and responsibilities of students and the consequences associated with cybersafety breaches that undermine the safety of the college environment.

All students must read and agree to abide by this policy before being able to use ICT equipment/ devices or access the internet on campus.

The **term 'ICT equipment & devices'** used in this document, includes, but is not limited to, computers (such as desktops, laptops, PDAs, tablets), storage devices (such as USB memory devices, CDs, DVDs, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, gaming consoles, video and audio players (such as portable CD and DVD players), and any other similar technologies as they come into use. Any images or material on personal devices must be appropriate to the college environment.

SECTION B Policy for use of internet and social media

Students must:

1. only use their own username and password to log on to the internet provided by the DPI. They must not allow others to use their log in details and not leave a logged-on computer unattended.
2. only use College ICT accounts and personal email accounts for approved purposes.
3. be aware that the College will use filtering and/or monitoring software to restrict access to certain sites and data, including email AND that ICT staff may monitor traffic, user screens and material sent and received using the DPI's ICT network.
4. *not* access, or attempt to access, inappropriate, age restricted or objectionable and offensive material (such as pornography, cruelty or violence that is incompatible with normal community standards, regardless of whether it is actual or generated by Artificial Intelligence, AI).
5. *not* download, save or distribute such material described above by copying, storing, printing, manipulating or generating by AI, or showing it to other people.
6. *not* attempt to get around or bypass security, monitoring and filtering that is in place.
7. report immediately any inappropriate material they or others come across by accident.
8. *not* download or install any files such as music, videos, games or programmes that may infringe copyright regulations.

9. *not* give out any private information (including photos) online about other students/staff, without their permission. Private information includes name, address, email address, phone numbers, photos and social media account access.
10. *not* copy any software or files (including photos) from the DPI network without permission from a staff member.
11. respect all ICT systems in use at the College and treat all ICT equipment/devices with care. This includes:
    - not intentionally disrupting the smooth running of any ICT systems
    - not attempting to gain unauthorised access to any restricted areas of the network or the personal data files of others.
    - leaving all computer settings and cabling as set by the IT staff
    - Scanning all storage media for viruses
    - reporting any potential security problems to a staff member
    - reporting any breakages/damage to a staff member immediately.
12. obey the privacy laws surrounding the capturing and sharing of images and video. Specifically, they will *not*:
    - capture photos or videos of members of the College community or at College-organised events without approval
    - post any such images or videos on any social networking and/or image/video sharing websites unless approved by staff
    - participate in any commenting in social networking conversations of a libellous nature about another member of the College community.
13. *not* participate in any commenting on social networking that would bring Tocal into disrepute.
14. *not* use ICT at College or elsewhere, to upset, offend, harass, threaten or harm anyone connected to the College community, or put themselves or anyone else at risk of this, even as a joke.
15. *not* post, publish, or share, AI generated or manipulated images of another person without their consent, and without acknowledging that the images have been altered.
16. *not* engage in cyber bullying behaviour directed to another member of the College community. This can be defined as: any material posted (in any form – photos, print) on a website or sent on the Internet or any technological device which identifies, bullies, embarrasses or harasses individual students, groups, parents and families, staff or others in the community. **This applies both at and away from the geographical College location using College or privately owned devices.** It can include:
    - Annoying/repeated phone calls
    - Harassing, offensive or obscene emails
    - Threatening emails or text messages
    - Defamatory, embarrassing or personal information on message boards or chat rooms
    - Posting information or photos without the victim's permission with the intent to cause hatred
17. *not* capture and/or post images, video, or other recordings of Tocal College and its activities without approval. This includes the unauthorised capture and/or sharing of training, social events, farming activities or assets on its campus, farm enterprises and host venues. These assets include, but are not limited to, infrastructure, machinery, and livestock.

Note: Students must provide their mobile number to staff and immediately advise any changes.

If a student is in breach of this policy, the College may inform parents/feepayers. In addition, they may incur other disciplinary actions. Any costs of repairs for damage to equipment will be charged to the student or feepayer. If illegal material or activities are involved, the police may be notified.

SECTION C Tocal Internet and Social Media Policy Agreement Form

TOCAL: Responsibilities include –

- **We will** do our best to keep the College cybersafe, by maintaining an effective Social Media program. This includes working to restrict access to inappropriate, harmful or illegal material on the Internet or ICT equipment/devices and enforcing the cybersafety rules and requirements detailed in this policy
- **We will keep** a copy this signed agreement on file
- **We will respond** appropriately to any breaches of the policy
- **We will welcome** enquiries from students or parents about cybersafety issues.

STUDENT: My responsibilities include -

- **I will read** the Social Media Policy carefully
- **I will follow** the cybersafety rules and instructions while I am a member of the Tocal community
- **I will** also follow the cybersafety rules whenever I use privately-owned ICT on or off the College while I am a student
- **I will avoid** any involvement with material or activities which could put at risk my own safety, or the privacy, safety or security of the College or other members of the Tocal community
- **I will take** proper care of College ICT AND I know that if I have been involved in the damage, loss or theft of ICT equipment/devices, my family may have responsibility
- **I will keep** this document somewhere safe so I can refer to it in the future
- **I will ask a staff member** if I am not sure about anything to do with this agreement.

I have read and understood my responsibilities and agree to abide by this Social Media Policy. I know that if I breach this Use Agreement there may be serious consequences.

………………………………………… ……………………………………………. ………………………
Student name Student signature Date

Mobile Phone Number: ……………………………………
(Students must advise staff of any change in phone number during their course)

PARENT / GUARDIAN (for students under 18): My responsibilities include -

- **I will read** this Social Media Policy Agreement carefully and discuss it with my son/daughter so we both have a clear understanding of their responsibilities in maintaining a Cybersafe environment.
- **I will encourage** my son/daughter to follow the Social Media Policy and instructions.
- **I will contact** the College if there is any aspect of this policy I would like to discuss.

………………………………………… ……………………………………………. ………………………
Parent name Parent signature Date