Nazareth
CATHOLIC COMMUNITY

Nazareth Catholic Community Staff Acceptable Use of Information and Communications Technology Procedures

INTRODUCTION

At Nazareth Catholic Community technology is used to support teaching, learning and for business purposes. With access to these resources come both privileges and responsibilities. Nazareth Catholic Community expects technology to be used in a safe, responsible, respectful and ethical manner at all times and these procedures should be read in conjunction with relevant SACCS policies and procedures especially *Protective Practices for staff in their interactions with children and young people* and *Code of Conduct for staff employed in Catholic Education SA*.

DEFINITIONS

NCC refers to Nazareth Catholic Community
CESA refers to Catholic Education South Australia
ICT refers to Information and Communications Technologies
Cloud Computing or **Cloud Services** involves the use of web-based services (rather than a PC or school server) for functions such as email, blogs, and lodgement of assignments and data storage.

STAFF RESPONSIBILITIES

1. The use of Nazareth Catholic Community ICT Facilities (including the use of Personal ICT Devices to access material on the network) should be consistent with the Catholic ethos and the values espoused by Catholic Education South Australia.

2. Using the Nazareth Catholic Community ICT Facilities or Personal ICT Devices that access material on the network and Cloud tenants are licensed by Nazareth Catholic Community.

<u>Interaction with others when using devices</u>

2.1. Staff must behave ethically and responsibly in all dealings with others.

<u>Privacy and Confidentiality</u>

Staff must:

2.2. Only obtain access to records or information that is relevant to their duties and that they have been authorised to access.
2.3. Observe obligations regarding confidentiality and privacy, for example, use BCC fields when sending emails to groups of parents to prevent recipients from seeing other recipients' email addresses.

Network Security Responsibilities

Staff must:

2.4. Ensure that they do not permit or facilitate unauthorised use of the Nazareth Catholic Community ICT Facilities by anyone.
2.5. Promptly report any evidence or reasonable suspicion of unauthorised access/use to the Nazareth Network Team.

Password and Device Security

Staff must:

2.6. Maintain a secure password and ensure that they do not provide the password to anyone else.
2.7. Use safeguards such as locking their computers (Shortcut key: Win + L for PCs) when physically away from their device.
2.8. Ensure that when personal devices that access material on Nazareth Catholic Community's network and services that they be protected with either a secure password, access code, pattern or PIN. e.g. Mobile phone must be passcode locked.

Access to Inappropriate Content

Staff must:

2.9. Promptly report any accidental access to inappropriate material to the Nazareth Network Team.
2.10. Use software installed by Nazareth Catholic Community for its intended use.

Nazareth Catholic Community Branding

Staff must:

2.11. Use the Nazareth Catholic Community Branding for email signatures.
2.12. Use the Nazareth Catholic Community Style Guide for all communication.

3. Nazareth Catholic Community ICT Facilities or Personal ICT Devices that access material on the network.

Interaction with others when using devices

Staff must not:

3.1. Send or publish any statement, image or other material that is offensive or threatening, or could constitute harassment, discrimination, vilification, defamation or cyberbullying.
3.2. Do anything that a user knows or reasonably suspects could contravene the law, including without limitation, downloading material in breach of copyright.

Access to Inappropriate Content

Staff must not:

3.3. Knowingly access, download, store, send or publish any material that is pornographic.
3.4. Send or help to send unsolicited bulk email (spam).
3.5. Engage in any online gambling.
3.6. Engage in any commercial activities, e.g.: running an online business.
3.7. Open or download any attachment, or access any link, that the staff member reasonably suspects may contain a virus or malware (any such attachment or link should be forwarded to the Nazareth Network Team for investigation).

Unauthorised access

Staff must not:

3.8. Obtain unauthorised access to Nazareth/CESA or any other network, or deliberately degrade the performance of the Nazareth/CESA data network or install any unlicensed or non-approved software onto computers or other communication devices supplied by Nazareth Catholic Community.
3.9. Attempt to gain unauthorised access to anyone else's account or user information, or otherwise attempt to defeat any security controls.
3.10. Use another person's email account or other means of communication to send any communication in that other person's name (unless specifically authorised by Leadership).

Privacy, Confidentiality and Device Care:

Staff must not:

3.11. Take photos or videos of members of Nazareth Catholic Community without their consent.
3.12. Store any documents, photo or information relating to Nazareth Catholic Community on their Personal ICT device.

Staff are:

3.13. Responsible for the physical control and safe keeping of any supplied device and are responsible for ensuring that other people do not access any confidential information contained on the device, or misuse the device.

4. Personal Use of Nazareth Catholic Community Devices

4.1. Staff may use Nazareth Catholic Community ICT Facilities for incidental personal use, provided such use is minimal and does not interfere with the performance of their duties.

5. Loss of Device

5.1. Staff must promptly report to Nazareth Leadership any loss of, or unauthorised access to, any personal or Community-owned communication devices that contain work-related information or information that is otherwise confidential to Nazareth Catholic Community.

6. Employment Conclusion

6.1. Upon conclusion of employment with Nazareth Catholic Community, staff must permanently remove from their Personal ICT Devices any work-related information, or information that is otherwise confidential to the school.

7. Monitoring of Device Use

7.1. Staff's appropriate use of Nazareth Catholic Community ICT Facilities (including Personal ICT Devices connected to the Network) will be monitored by the Nazareth Network Team, and any evidence of use that contravenes this practice, or is otherwise inappropriate, may lead to disciplinary consequences in accordance with the section *Consequences of Non-Compliance* contained within this document.

7.2. In the case of an investigation into the conduct of a staff member, the staff member must if requested, provide his or her Nazareth device/s to Nazareth Catholic Community Leadership (together with any information such as passwords that is necessary to gain full access to the devices) for the purposes of assisting the authorities to determine whether inappropriate conduct has occurred.

8. Use of Social Media by Staff

8.1. When posting material in a social media forum (e.g. Facebook page, Twitter, blogs) staff should be aware that such activity may be considered public, not private.

Nazareth Catholic Community staff must not:

8.2. Connect or interact with students through social media (e.g. Facebook friends or Facebook private messages) without the written consent of Nazareth Leadership, other than in the case of any social media site specifically created or provided by the Nazareth Catholic Community for the purpose of facilitating online communication between staff and students.

8.3. Divulge any confidential information, including students' personal information, through social media.

8.4. If someone else posts a comment or other material in a staff members' Social Media space, if that comment or material:

- Is likely to cause serious damage to the relationship between Nazareth Catholic Community and the staff member or
- Is likely to damage the interests of Nazareth Catholic Community or
- Is incompatible with the staff members' duty to Nazareth Catholic Community.

The staff member must (where possible) remove that comment or material as soon as it comes to their attention and if possible provide a copy to Nazareth Catholic Community Leadership.

8.5. Staff accessing a public network (internet) on a Nazareth device not managed by the Nazareth Catholic Community must comply with this Acceptable Use Practice; furthermore, when connected to the public network the computing device shall not be simultaneously connected to the CESA network, unless connected through a CESA ICT approved network access facility (VPN).

8.6. Staff must not copy confidential information to sites outside of the Nazareth Catholic Community without prior authorisation.

CONSEQUENCES OF NON-COMPLIANCE

In the event that a staff member is found to have breached the ICT Acceptable Use Policy, consequences may include:

- Verbal counselling or warning
- Formal written warning
- Formal final warning or
- Dismissal.

Any investigation will be carried out in accordance with the SACCS 2005 document: Procedures for Dealing with Allegations of Misconduct. Evidence of illegal conduct will be reported to SAPOL or the Australian Federal Police.

Responsibilities of Nazareth Catholic Community as an organisation

The additional responsibilities of Nazareth Catholic Community in relation to ICT Acceptable Use are to:

- Educate students about the use of technology and the risks involved in that use, including the potential inaccuracy of online information, ways to check the authenticity of information and strategies to stay safe online
- Use appropriate software supplied by Nazareth Catholic Community to ensure positive use of all Nazareth Catholic Community ICT Facilities
- Work with Leadership to implement regular information and education sessions for students (and where appropriate, parents) to promote understanding of available technologies, the benefits of, and inherent risks involved in, use of those technologies, and the content of the Acceptable Use Agreement
- Promptly report to Nazareth Catholic Community Leadership any known or suspected breaches of the community's Acceptable Use Agreement that may constitute a criminal offence.

NAZARETH CATHOLIC COMMUNITY LEADERSHIP RESPONSIBILITIES

The additional responsibilities of Nazareth Catholic Community Leadership in relation to ICT Acceptable Use are to:

- Implement appropriate measures to enable compliance with these practices to be monitored, and to enable any breaches to be detected
- Update this Acceptable Use of Information and Communications Technology Policy on an annual basis or as the need arises.
- Ensure all staff and students (and parents in the case of students under the age of 18 years) sign the Acceptable Use Agreement at the beginning of each school year (or when the staff member or student joins the School, if part-way through the year)
- Ensure appropriate storage of the Acceptable Use of Information and Communications Technology Agreement.

- Ensure regular professional development sessions are conducted and informal reminders are issued to staff in relation to the schools Acceptable Use of Information and Communications Technology Agreement and that new staff are made aware of the Acceptable Use of Information and Communication Technology Agreement as part of their induction process.
- Ensure regular information and education sessions are held for students (and where appropriated, parents) to promote understanding of available technologies, the inherent risks involved in use of those technologies and the content of the Acceptable Use of Information and Communication Technology Agreement.
- Promptly report to the Director any known or suspected breaches of the school's Acceptable Use of Information and Communication Technology Agreement that may constitute a criminal offence.

CONCLUSION

The terms of this document are not intended to be exhaustive, nor do they anticipate every possible use of the Nazareth Catholic Community ICT Facilities. Staff are encouraged to act responsibly and take into account the principles underlying ICT Acceptable Use.