ACCEPTABLE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICY

(BASELINE STANDARD)

VISION

Catherine McAuley School is a Catholic Faith community which promotes and celebrates excellence in education.

A spirit of reconciliation is encouraged through our experience of faith, growth and unity.

We endeavour to prepare children for a life that is lived in justice, dignity and mutual respect.
1 INTRODUCTION
The South Australian Commission for Catholic Schools (SACCS) acknowledges the increasing use of information and communications technologies as a learning and business tool in schools. SACCS celebrates the capacity of the new technologies including mobile communication devices and the use of social media to foster and support positive relationships and various forms of harmony through the promotion of a culture where there is respect for all and where all are invited to search for truth in dialogue. SACCS encourages communities to develop reflective and responsible practices around their use of electronic technologies and the internet.

Information and communications technology is to be used to enhance the quality of human life, whether in an educational, social, recreational or work context. At the school, technology is mostly used to support teaching and learning and for business purposes. Catholic Education South Australia (CESA) expects technology to be used in a safe, responsible, respectful and ethical manner at all times.

2 DEFINITIONS

CEO
either or both of the Adelaide and Port Pirie Catholic Education Offices, as the context permits.

CESA
Catholic Education SA, including any School or CEO, as the context may permit.

CESA ICT Facilities
include computer systems, cloud based resources, data networks, wireless infrastructure, internet connections, computers, laptops, smart phones, other devices, applications and printers and other means of electronic communication provided by the Workplace.

Cyberbullying
is the use of the Internet and related technologies to harm other people, in a deliberate, repeated, and hostile manner.

Personal ICT Device or BYOD
a device owned, leased or otherwise used by an individual that is not provided by the employer but is capable of accessing material on the Workplace's network and services, or is capable of acting as a Wifi hotspot.

School
Catherine McAuley School /any South Australian Catholic school.
**Social Media** refers to a range of online services and tools used for publishing, sharing and promoting interaction and dialogues.

**Workplace** means the School in the case of Workplace Participants working or volunteering at a South Australian Catholic school, and means the CEO in the case of other Workplace Participants.

**Workplace Participants** means:

a. employees, consultants, contractors and volunteers of any School or CEO;

b. office holders (including of SACCS, SACCS committees, School Boards, School Governing Councils and the Federation of Catholic School Parent Communities); and

c. clergy, religious and parish workers to the extent that they are using CESA ICT Facilities.

### 3 SCOPE OF POLICY

This Policy is designed to promote the acceptable use of electronic information and communications technology by all Workplace Participants.

This Policy covers the:

- use of CESA Information and Communications Technology (ICT) Facilities (whether within or outside of normal working hours, and whether on or off site), including use of CESA networks/internet connections to access the internet using Personal ICT Devices (whether within or outside of normal working hours), and including remote access

- other use of Personal ICT Devices (including outside of normal working hours and including when off-site) where such use:
  - is likely to cause serious damage to the relationship between the School/CEO and the Workplace Participant or
  - is likely to damage the interests of the School/CEO or
  - is incompatible with the Workplace Participant’s duty to the School/CEO.
4 RESPONSIBILITY FOR IMPLEMENTATION, MONITORING AND CONTINUAL IMPROVEMENT

4.1 Responsibilities of All Workplace Participants

4.1.1 The use of CESA ICT Facilities (including the use of Personal ICT devices to access material on the Workplace's network and services) should be consistent with the Catholic ethos and the values espoused by Catholic Education South Australia. Any reference to Catholicism, Catholic Church, Catholic schools, Pope, the Bishop and other clergy must be consistent with obligations to uphold the Catholic ethos.

4.1.2 In using the CESA ICT Facilities or Personal ICT devices that access material on the Workplace's network and services, Workplace Participants must:

4.1.2.1 behave ethically and responsibly in all dealings with others
4.1.2.2 only obtain access to records or information that is relevant their duties and have been authorised to access
4.1.2.3 observe obligations regarding confidentiality and privacy
4.1.2.4 maintain a secure password and ensure that they do not provide the password to anyone else
4.1.2.5 not attempt to gain unauthorised access to anyone else’s account or user information, or otherwise attempt to defeat any security controls
4.1.2.6 not 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 that person)
4.1.2.7 not take photos or video of members of the school community without their consent
4.1.2.8 ensure that they do not permit or facilitate unauthorised use of the CESA ICT Facilities by anyone
4.1.2.9 promptly report any evidence or reasonable suspicion of unauthorised access/use to the School or CEO authorities and
4.1.2.10 promptly report any accidental access to inappropriate material.
4.1.3 CESA ICT Facilities or Personal ICT devices that access material on the Workplace’s network and services should not be used to:

4.1.3.1 send or publish any statement, image or other material that is offensive or threatening, or could constitute harassment, discrimination, vilification, defamation or cyberbullying

4.1.3.2 knowingly access, download, store, send or publish any material that is pornographic

4.1.3.3 do anything that the user knows or reasonably suspects could contravene the law, including without limitation downloading material in breach of copyright

4.1.3.4 send or help to send unsolicited bulk email (spam)

4.1.3.5 open or download any attachment, or access any link, that the Workplace Participant reasonably suspects may contain a virus, malware or other computer contaminant (any such attachment or link should be forwarded to the Workplace ICT personnel for authentication)

4.1.3.6 obtain unauthorised access to the School/CEO or any other network, or to deliberately degrade the performance of the School/CEO data network or

4.1.3.7 install any unlicensed or non-approved software onto computers or other communication devices supplied by the School or CEO

4.1.4 Workplace Participants are responsible for the physical control and safe keeping of any laptops, mobile telecommunication devices, and other communication devices supplied to them by the School/CEO, and are responsible for ensuring that other people do not access any confidential information contained on the device, or misuse the device.

4.1.5 Workplace Participants may use CESA ICT Facilities for incidental personal use, provided such use is minimal and does not interfere with the performance of their duties, but are not permitted to use CESA ICT Facilities to store or download large files (including music or movies) for personal use. All personal use of CESA ICT Facilities must conform to this practice.

4.1.6 Personal devices that access material on the Workplace’s network and services must be protected with a secure password, access code, pattern or PIN.
4.1.7 Workplace Participants must promptly report to the School/CEO authorities any loss of, or unauthorised access to, any communication devices that contain work-related information or information that is otherwise confidential to the School/CEO.

4.1.8 Where a device that contains CESA data is lost or stolen School/CEO authorities reserve the right to erase all data on the device including any personal data.

4.1.9 Upon conclusion of their role within the School/CEO, Workplace Participants must permanently remove from their Personal ICT Devices any work-related information, or information that is otherwise confidential to the School/CEO.

4.1.10 Workplace Participants’ use of CESA ICT Facilities (including Personal ICT devices that are used to access material on the Workplace's network and services) may be monitored by School and/or CEO personnel, and any evidence of use that contravenes this practice, or is otherwise inappropriate, may lead to disciplinary consequences in accordance with ‘Section 4.4 Consequences of Non-Compliance’. In the case of an investigation into the conduct of a Workplace Participant, the Workplace Participant must, if requested, provide his or her Personal ICT devices to the School/CEO authorities (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.

4.1.11 When posting material in a Social Media forum (eg Facebook page, Twitter, blogs) Workplace Participants should be aware that such activity may be considered public, not private.
4.1.12 Workplace Participants must not:

4.1.12.1 connect or interact with students through Social Media (eg Facebook friends or Facebook private messages) without the Principal’s written consent, other than in the case of any Social Media site specifically created or provided by a School (and authorised by the Principal) for the purpose of facilitating online communication between Workplace Participants and students; or

4.1.12.2 divulge any confidential information, including students’ personal information, through Social Media.

4.1.13 If someone else posts a comment or other material in a Workplace Participant’s Social Media space, then if that comment or material:

4.1.13.1 is likely to cause serious damage to the relationship between the School/CEO and the Workplace Participant or

4.1.13.2 is likely to damage the interests of the School/CEO or

4.1.13.3 is incompatible with the Workplace Participant’s duty to the School/CEO,

the Workplace Participant must (where possible) remove that comment or material as soon as it comes to their attention.

4.1.14 Workplace Participants accessing a public network (Internet) not managed by the school / CEO must comply with this Acceptable Use of Information and Communications Technology Policy (Baseline Standard); 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.

4.2 Responsibilities of Principals

The additional responsibilities of Principals in relation to ICT Acceptable Use are to:

4.2.1 implement appropriate measures in his or her School to enable compliance with these practices to be monitored, and to enable any breaches to be detected
4.2.2 ensure that on an annual basis, promptly at the commencement of each school year, his or her School prepares and implements an Acceptable Use of ICT Agreement incorporating all of the matters set out in Appendix A

4.2.3 encourage participation of students, parents and staff in the preparation of the Acceptable Use of ICT Agreements

4.2.4 ensure that all Workplace Participants and students (and parents in the case of students under the age of 18 years) sign the Acceptable Use of ICT Agreement at the beginning of each school year (or when the Workplace Participant or student joins the school, if part-way through the year)

4.2.5 ensure appropriate storage of the Acceptable Use of ICT Agreements

4.2.6 ensure regular professional development sessions are conducted and informal reminders are issued to Workplace Participants in relation to the School’s Acceptable Use of ICT Agreement and Acceptable Use of Information and Communications Technology Policy (Baseline Standard), and that new Workplace Participants are made aware of the Acceptable Use of Information and Communications Technology Policy (Baseline Standard) and the ICT Acceptable Use Agreement as part of their induction process

4.2.7 ensure regular information and education sessions are held for students (and where appropriate, parents) to promote understanding of available technologies, the inherent risks involved in use of those technologies, and the content of the Acceptable Use of ICT Agreement

4.2.8 promptly report to the Principal Consultant (and in the case of congregationally governed schools and schools governed by Catholic Special Schools Incorporated, the Principal’s employing authority) any known or suspected breaches of the school’s Acceptable Use of Information and Communications Technology Policy (Baseline Standard) and Acceptable Use of ICT Agreement that may constitute a criminal offence.
4.3 Responsibilities of School Staff

The additional responsibilities of school Workplace Participants in relation to ICT Acceptable Use are to:

4.3.1 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

4.3.2 work with the Principal 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 of ICT Agreement

4.3.3 promptly report to the Principal any known or suspected breaches of the school’s Acceptable Use of Information and Communications Technology Policy (Baseline Standard) and Acceptable Use of ICT Agreement that may constitute a criminal offence.

4.4 Consequences of Non-Compliance

In the event that a Workplace Participant is found to have breached the Acceptable Use of Information and Communications Technology Policy (Baseline Standard) or Acceptable Use of ICT Agreement, consequences may include:

- verbal counselling or warning
- written counselling or warning
- formal final warning or
- dismissal

as well as limitation or suspension of some or all of the Workplace Participant’s right to use CESA ICT Facilities.

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 (as appropriate).
4.5 **Conclusion**

The terms of this Policy are not intended to be exhaustive, nor do they anticipate every possible use of the School's or CEO's ICT Facilities. Workplace Participants are encouraged to act responsibly and take into account the principles underlying ICT Acceptable Use.

5 **RELATED POLICIES, PROCEDURES and RESOURCES**

The following documents are to be read in conjunction with this Policy.

- SACCS Information and Communications Technology Security Policy
- SACCS Information and Communications Technology Security Framework
- Catherine McAuley School: Code of Conduct for Staff

**DATE FOR REVIEW**

**Reviewed:** 4 November 2015  
**Next Review:** 2020

*Please Note: This Policy is informed by the SACCS ‘Acceptable Use of Information and Communications Technology Baseline Standard V2.0’ and is due for revision by SACCS in April 2017.*

The school will follow any updates (prior to the next scheduled revision date by the school) as per SACCS advice.
**Appendix A - Checklist of items to be covered in Acceptable Use of Information and Communications Technology (ICT) Agreements.**

**CHECKLIST OF MATTERS TO BE COVERED IN SCHOOLS’ ACCEPTABLE USE of ICT AGREEMENTS**

*Exact wording and concepts to be adapted to suit the age and development of the relevant students in each School context.*

<table>
<thead>
<tr>
<th>1. <strong>Scope of Acceptable Use of ICT Agreements</strong> <em>(refer to Section 3 of this Policy)</em></th>
<th>□</th>
</tr>
</thead>
<tbody>
<tr>
<td>with particular emphasis on use of personal devices at school, and out of hours conduct (e.g. no cyber bullying or derogatory comments about school, Workplace Participants or other students)</td>
<td></td>
</tr>
<tr>
<td>The Acceptable Use of ICT Agreements cover:</td>
<td></td>
</tr>
<tr>
<td>• all students and Workplace Participants of the School</td>
<td></td>
</tr>
<tr>
<td>• all use of School ICT facilities</td>
<td></td>
</tr>
<tr>
<td>• all use of Personal ICT devices to access the School’s network or facilities</td>
<td></td>
</tr>
<tr>
<td>• conduct both during and outside of school hours.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. <strong>Acceptable Conduct</strong> <em>(refer to Section 4.1 of this Policy)</em></th>
<th>□</th>
</tr>
</thead>
<tbody>
<tr>
<td>• conduct consistent with the Catholic ethos</td>
<td></td>
</tr>
<tr>
<td>• behave ethically and responsibly in all dealings with others</td>
<td></td>
</tr>
<tr>
<td>• observe obligations regarding confidentiality and privacy</td>
<td></td>
</tr>
<tr>
<td>• select and maintain a secure password and ensure you do not provide the password to anyone else</td>
<td></td>
</tr>
<tr>
<td>• not attempt to gain unauthorised access to anyone else’s account or user information, or otherwise attempt to defeat any security controls</td>
<td></td>
</tr>
<tr>
<td>• not 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 that person)</td>
<td></td>
</tr>
<tr>
<td>• restrictions on use of devices that record others or take photos</td>
<td></td>
</tr>
<tr>
<td>• report any suspicions of unauthorised or inappropriate access to the school or CEO authorities</td>
<td></td>
</tr>
<tr>
<td>• treating equipment with care</td>
<td></td>
</tr>
<tr>
<td>• physical control and safe keeping of devices supplied to them by the School</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. <strong>Unacceptable Conduct</strong></th>
<th>□</th>
</tr>
</thead>
<tbody>
<tr>
<td>• send or publish any statement, image or other material that is offensive or threatening, or could constitute harassment, discrimination, vilification, defamation or cyberbullying</td>
<td></td>
</tr>
<tr>
<td>• knowingly access, download, store, send or publish any material that is pornographic</td>
<td></td>
</tr>
<tr>
<td>• do anything that you know or reasonably suspect could contravene the law, including without limitation downloading material in breach of copyright</td>
<td></td>
</tr>
<tr>
<td>• send or help to send unsolicited bulk email (spam)</td>
<td></td>
</tr>
<tr>
<td>• open or download any attachment, or access any link, that you reasonably suspect may contain a virus, malware or other computer contaminant (any such attachment or link should be forwarded to the Workplace ICT personnel for authentication)</td>
<td></td>
</tr>
<tr>
<td>• hack into the School/CEO or any other network, or deliberately degrade the performance of the School/CEO data network or</td>
<td></td>
</tr>
<tr>
<td>• install any unlicensed or non-approved software onto computers or other communication devices supplied by the School or CEO</td>
<td></td>
</tr>
<tr>
<td>• use ICT devices to cheat or plagiarise</td>
<td></td>
</tr>
<tr>
<td>• use CESA ICT Facilities to store or download large files (including music or movies) for personal use; all personal use of CESA ICT Facilities must conform with this practice</td>
<td></td>
</tr>
</tbody>
</table>

| 4. **Staying Safe Online** Reporting to an adult if a student accesses a website or sees something online that makes him or her feel uncomfortable | □ |

| 5. **Specifics of what to do in the event of cyberbullying** *(victims and bystanders)* | □ |
6. **Personal Devices** *(refer to Section 2 of this Policy)*

Users of personal devices are responsible for these devices and must not rely on the school’s insurance to cover damage or loss.

Personal ICT devices that access material on the School’s network and services:
- must be protected with a secure password
- may be monitored by School and/or CEO personnel
- must be provided to the School/CEO authorities for the purposes of assisting the authorities to determine whether inappropriate conduct has occurred.

Personal ICT devices should not be used to:
- send or publish any statement, image or other material that is offensive or threatening, or could constitute harassment, discrimination, vilification, defamation or cyberbullying
- knowingly access, download, store, send or publish any material that is pornographic
- do anything that the user knows or reasonably suspects could contravene the law, including without limitation downloading material in breach of copyright or the intellectual property rights of others without appropriate approval
- send or help to send unsolicited bulk email (spam) without the specific consent of the Principal or manager
- open or download any attachment, or access any link, that the Workplace Participant reasonably suspects may contain a virus, malware or other computer contaminant (any such attachment or link should be forwarded to the Workplace ICT personnel for authentication)
- hack into the School/CEO or any other network, or to deliberately degrade the performance of the School/CEO data network or
- install any unlicensed or non-approved software onto computers or other communication devices supplied by the School or CEO

Students accessing a public network (Internet) not managed by the school / CEO 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.

7. **Students may use CESA ICT Facilities for incidental personal use**, provided such use is minimal and does not interfere with the performance of their duties.

8. **Students are encouraged to collaborate within the system**, however this should be done in a safe manner; Students should obtain a teacher’s permission prior to establishing contact with participants not associated with their school, teachers should record any approvals granted for external collaboration.

9. **When posting material in a Social Media forum** *(eg Facebook page, Twitter, blogs)* **students should be aware that such activity may be considered public, not private.**

Limitations on what students can post in a social media forum, and what they should do if something inappropriate is posted on their page/site.

10. **Consequences** Consequences of breach of the Acceptable Use of ICT Agreement

11. **Additional responsibilities** Note that Workplace Participants are also bound by the ICT Acceptable Use of Information and Communications Technology Policy *(Baseline Standard)* and the Workplace Participant User Agreement.
This User Agreement sets out the terms on which you may access ICT facilities provided by the School / SACCS and cloud computing services, including Microsoft O365, iScholaris, Edmodo, Edublogs, Google Apps and [insert name] (Cloud Computing Services). Cloud computing involves the use of web-based services (rather than a PC or school server) for functions such as email, blogs, lodgement of assignments and data storage.

You will need to sign and return this User Agreement before you will be allowed to access these Services.

By signing this User Agreement, you (including parents/guardians in the case of students under 18 years) are agreeing to the terms set out in this User Agreement, including the consequences of any breach of the terms.

1. Privacy Consent

   Information that you transfer or store using the school’s Cloud Computing Services (including email, assignments, blogs and data storage) may be stored by Microsoft O365, iScholaris, Edmodo, Edublogs, Google Apps or other Cloud Computing Service providers (Cloud Providers) in the United States of America, or such other country as the Cloud Providers may decide. By using the School’s Cloud Computing Services, you are consenting to the transfer to, and processing and storage of your information in, such overseas location, even though the privacy laws in those countries may be different to the privacy laws in Australia.

2. Acceptable Use

   You agree that you will comply with all requirements as set out in this User Agreement and in the Acceptable Use of Information and Communications Technology (Baseline Standard) and all other relevant laws and restrictions in your access to the various information and communication technology resources through the school and SACCS network (including email, the Internet, cloud computing services and services provided through third parties), that you will not use the Cloud Computing Services to do anything that is against the law, and that you will not:

   (a) send or help to send unsolicited bulk email (spam);
   (b) publish material that is hurtful or offensive to other people, including material that is defamatory, threatening or discriminatory;
   (c) knowingly create or send any viruses, worms, Trojan horses or anything of a similar nature; or
   (d) disable, change, reverse-engineer or otherwise interfere with the Cloud Computing Services.

   Students are required to obtain teacher permission prior to establishing contact with participants not associated with their school.
3. Monitoring
You agree that School Workplace Participants and Catholic Education Office Workplace Participants responsible for ICT systems will have the ability to (and may at any time) monitor your use of the Cloud Computing Services, including accessing and monitoring any data that you have sent or stored using the Cloud Computing Services, to ensure that you are using the Cloud Computing Services appropriately.

4. Suspension or termination of use and other consequences
If there is an emergency security issue, or if you are suspected of making inappropriate use of the Cloud Computing Services, your access to the Cloud Computing Services may be suspended or terminated. This means that you might not be able to access your school email, assignments, blogs and data storage. If you are found to have made inappropriate use of the Cloud Computing Services, the School may also apply other disciplinary consequences.

Agreement and Consent
I, the student named below hereby agree to comply with all requirements as set out in this User Agreement and in the Acceptable Use of Information and Communications Technology Policy (Baseline Standard) and all other relevant laws and restrictions in my access to the various information and communication technology resources through the School and SACCS network (including email, the Internet, Cloud Computing Services and services provided through third parties).

NAME: ____________________________________ CLASS: ______

SIGNATURE: _______________________________ _ DATE: ______

Parent/Guardian Consent (for students under 18 years of age)
As the parent or legal guardian of the student named above, I consent to the student accessing the various information and communication technology resources through the School and SACCS network (including email, the Internet, Cloud Computing Services and services provided through third parties) on the terms set out in this User Agreement and in the Acceptable Use of Information and Communications Technology Policy (Baseline Standard) and all other relevant laws and restrictions.

NAME: ____________________________________ DATE: ______

SIGNATURE: _______________________________ _
WORKPLACE PARTICIPANTS [INSERT YEAR]
ACCEPTABLE USE OF ICT AGREEMENT

[INSERT SCHOOL NAME]

This User Agreement sets out the terms on which you may access ICT facilities provided by the School / SACCS and cloud computing services, including Microsoft O365, iScholaris, Edmodo, Edublogs, Google Apps and [insert name] (Cloud Computing Services). Cloud computing involves the use of web-based services (rather than a PC or school server) for functions such as email, blogs, lodgement of assignments and data storage.

You will need to sign and return this User Agreement before you will be allowed to access these Services.

By signing this User Agreement, you (including parents/guardians in the case of students under 18 years) are agreeing to the terms set out in this User Agreement, including the consequences of any breach of the terms.

1. Privacy Consent

Information that you transfer or store using the school’s Cloud Computing Services (including email, assignments, blogs and data storage) may be stored by Microsoft O365, iScholaris, Edmodo, Edublogs, Google Apps or other Cloud Computing Service providers (Cloud Providers) in the United States of America, or such other country as the Cloud Providers may decide. By using the School’s Cloud Computing Services, you are consenting to the transfer to, and processing and storage of your information in, such overseas location, even though the privacy laws in those countries may be different to the privacy laws in Australia.

2. Acceptable Use

You agree that you will comply with all requirements as set out in this User Agreement and in the Acceptable Use of Information and Communications Technology (Baseline Standard) and all other relevant laws and restrictions in your access to the various information and communication technology resources through the School and SACCS network (including email, the Internet, cloud computing services and services provided through third parties), that you will not use the Cloud Computing Services to do anything that is against the law, and that you will not:

(a) send or help to send unsolicited bulk email (spam);

(b) publish material that is hurtful or offensive to other people, including material that is defamatory, threatening or discriminatory;

(c) knowingly create or send any viruses, worms, Trojan horses or anything of a similar nature; or

(d) disable, change, reverse-engineer or otherwise interfere with the Cloud Computing Services.
3. **Monitoring**

You agree that School Workplace Participants and Catholic Education Office Workplace Participants responsible for ICT systems will have the ability to (and may at any time) monitor your use of the Cloud Computing Services, including accessing and monitoring any data that you have sent or stored using the Cloud Computing Services, to ensure that you are using the Cloud Computing Services appropriately.

4. **Suspension or termination of use and other consequences**

If there is an emergency security issue, or if you are suspected of making inappropriate use of the Cloud Computing Services, your access to the Cloud Computing Services may be suspended or terminated. This means that you might not be able to access your school email, assignments, blogs and data storage. If you are found to have made inappropriate use of the Cloud Computing Services, the School may also apply other disciplinary consequences.

5. **Process and Storage of Certain Records**

You must not, without the specific written consent of the School Principal, use the Cloud Computing Services for the long term or permanent storage or retention of any of the following School records:

(a) taxation records including records relating to payroll tax and fringe benefits tax;
(b) employee records under applicable industrial legislation;
(c) workers compensation records
(d) medical records;
(e) records relating to occupational health, safety and welfare laws (including occupational health, safety and welfare policies and procedures and any documents relating to injuries suffered in the course of employment); and
(f) school attendance records.

---

**Agreement and Consent**

I, the Workplace Participant named below hereby agree to comply with all requirements as set out in this User Agreement and in the Acceptable Use of Information and Communications Technology (Baseline Standard) and all other relevant laws and restrictions in my access to the various information and communication technology resources through the School and SACCS network (including email, the Internet, Cloud Computing Services and services provided through third parties).

NAME: __________________________________________

SIGNATURE: _______________________________ _ DATE: ____

---

M:\Policy Masters\Admin\Acceptable Use of Information and Communications Technology Policy_Baseline Standard_November 2015.docx  Page 1 of 16