USE OF SERVICE DELIVERY ICT - PROTOCOLS

<table>
<thead>
<tr>
<th>Policy Area</th>
<th>Information Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document type</td>
<td>Protocols</td>
</tr>
<tr>
<td>Applicable to</td>
<td>Centacare Community Services</td>
</tr>
<tr>
<td>Version</td>
<td>1.0</td>
</tr>
<tr>
<td>Date approved</td>
<td>29 April 2016</td>
</tr>
<tr>
<td>Approved by</td>
<td>Senior Director</td>
</tr>
<tr>
<td>Review date</td>
<td>29 April 2017</td>
</tr>
<tr>
<td>Policy Sponsor</td>
<td>General Manager SSD</td>
</tr>
</tbody>
</table>

Related policy
- Archdiocesan Employment Policies:
  - Workplace Harassment
  - Sexual Harassment
  - Child Safety
  - Staff Separation including Counselling/Discipline
  - Code of Conduct
  - Use of Communication Mediums
  - Privacy Policy
  - Social Media
- Archdiocesan IT Security Policy
- Archdiocesan Back Up Policy
- Archdiocesan ICT Electronic (Email) Policy
- Centacare Privacy Policy
- Centacare – Data Breach Procedure
- CCS Policy – Records Management
- CCS Policy – Incident Reporting and Investigation

PURPOSE

The purpose of these Protocols is to define acceptable, safe and secure standards for the use and management of Centacare supplied communication and computing devices.

Centacare Community Services (CCS) is committed to the correct and proper use of communication and computing devices in support of its service delivery and business functions. The inappropriate use of communication and computing devices could expose Centacare to risks including, theft and/or disclosure of information, disruption of services, fraud or litigation.

These Protocols are mandatory and by using any communication and computing device which is owned or operated by the Centacare, Users are agreeing to abide by the terms of these Protocols.

Access by authorised personnel to communication and computing devices owned or operated by Centacare imposes certain responsibilities and obligations and is granted subject to the policies and procedures of the Archdiocese, including Centacare and Centacare Community Services, as listed above.
Centacare may withdraw a Centacare supplied communication and computing device from any employee who it believes is not complying with these Protocols or who misuses a Centacare supplied communication and computing device in any manner.

**SCOPE**

These Protocols apply to:

- all Centacare Community Services Support Workers issued with a Centacare supplied communication and computing device ("TRACCS Mobile Device") to implement the "TRACCS Time and Attendance App"; and
- any staff accessing or using a Centacare supplied computer, printer/scanner and/or wireless internet connection installed in a Supported Accommodation environment as a result of “the Computers in Houses” project.

1. **ISSUE AND MAINTENANCE**

1.1 Centacare Community Services is implementing projects that will provide:

- Support Workers with a “TRACCS Mobile Device” in order to implement the “TRACCS Time and Attendance App”; and
- networked docked computers and a wireless internet connection in Supported Accommodation environments.

1.2 TRACCS Mobile Devices will be issued to Support Workers by the CIMS team in liaison with the relevant Service. The issue of each Device will be registered and tracked by the Manager Property and Procurement.

1.3 Support will be available to Users through:

- referring to the Trouble Shooting Guide;
- seeking advice from Technology Mentors/Coordinators within each Service;
- seeking assistance, which will be provided using Team Viewer (software that enables remote access to a User's device) support, from:
  - CIMs - for TRACCS Mobile Device Users
  - Archdiocesan ICT - for Computers in Houses.

2. **OWNERSHIP**

2.1 Centacare supplied communication and computing devices will at all times remain the property of Centacare.

2.2 Centacare owns the rights to all data and files in any Centacare supplied communication and computing device, computer, network, or other information system used in Centacare and to all data and files sent or received using any Centacare device, system or any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property.
3. MONITORING

3.1 Centacare may monitor:

- the volume of data and telephone usage for Centacare accounts and networks;
- the location of a Centacare supplied communication and computing devices; and/or
- electronic communications (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of Centacare supplied communication and computing devices or Centacare networks.

3.2 Centacare may use software in its electronic information systems that allows monitoring by authorised personnel and that can be identify the location of a device and/or creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems.

3.3 Employees must be aware that all electronic communications sent and received using Centacare supplied devices, data accounts and networks are not private and may be subject to viewing, downloading, inspection, release, and archiving by Centacare at any time. Centacare may inspect any and all files stored in private areas of the network or on Centacare supplied communication and computing devices and storage media in order to assure compliance with Centacare's policies and state and federal laws.

3.4 Employees have no expectation of privacy in any information or activity conducted, sent, performed, or viewed on or with Centacare supplied devices, data accounts and networks. Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on a Centacare supplied communication and computing device or when using a Centacare supplied network may be electronically stored and subject to inspection, monitoring, evaluation, and Centacare use at any time.

3.5 Employees who use Centacare supplied communication and computing devices, data accounts and networks to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure. Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than Centacare supplied mobile phones/tablets and electronic communication devices, data accounts and networks.

3.6 While Centacare does not routinely monitor or access an individual User's communication and computing device activity, it may do so when there is a concern about staff safety or a breach of its policies and protocols or illegal activity is suspected. This monitoring may include but is not limited to details of location of the device, telephone calls made, messages and emails sent to and from the device, internet access, browsing history and information stored on the Centacare supplied communication and computing device.

3.7 The monitoring of an individual User's communication and computing device activity must be authorised by the relevant Stream or Regional Manager, General Manager, Director or the
Senior Director. The results of all monitoring will be stored securely and will only be shared with those authorised to have access to such information.

4. USAGE

4.1 Centacare supplied communication and computing devices are supplied primarily for Centacare work-related purposes.

4.2 All use of Centacare supplied communication and computing devices, including personal use, must be in accordance with the Policies, Procedures, Guidelines and Protocols of the Archdiocese, Centacare and Centacare Community Services including the Code of Conduct and Code of Ethical Behaviour.

4.3 Users must make every reasonable effort to ensure that their Centacare supplied communication and computing device is secured at all times, kept charged and switched on during working hours.

4.4 All communications including telephones calls, texts and emails should be answered in a clear, friendly and professional manner.

5. PERSONAL USE:

5.1 Reasonable Personal Use is permitted for telephones calls, email, internet browsing and; for mobile phones/tablets taking personal photos and audio-visual recordings. Personal use is a benefit and not a right.

5.2 Personal use of Centacare supplied communication and computing devices must be in a manner which is lawful, ethical and in accordance with Centacare’s Policies and Procedures including the Code of Conduct and Code of Ethical Behaviour.

5.3 Personal email and other electronic communications using a Centacare supplied communication and computing device must be made from personal addresses and accounts and must comply with Archdiocesan Employment Policy Social Media Use and Archdiocesan Employment Policy Use of Communication Mediums. There must be no suggestion that the communication is made on behalf of the Archdiocese, Centacare or Centacare Community Services.

5.4 “Apps” may be added to mobile phones/tablets. However, only Archdiocesan Information, Communications and Technology may install software on Centacare laptops and computers.

5.5 Excessive personal use of any communication and computing devices during working hours is not permitted. Personal use of any communication and computing device must not interfere with performance of duties and should generally only occur when the User is not on duty/working. Flexibility will be provided in circumstances demanding immediate attention, i.e. family emergencies.

5.6 Centacare supplied communication and computing devices may only be used by the authorised User/s and must not be used by third parties (such as a User’s family member) without the prior authorisation of the Manager.
5.7 An exception to 5.6 above is clients who live in supported accommodation are able to access the Centacare supplied wi-fi network on their own devices.

5.8 In the event that Centacare supplied communication and computing devices are lost, stolen, replaced, assigned to another User or sent for repair the contents of the device will be wiped. Centacare will not take any responsibility for loss of a User's personal information and files such as contact lists, photos, audio-visual files etc.

6. RESTRICTIONS ON USAGE

6.1 Telephones calls made from a Centacare supplied mobile phone/tablet must be restricted to local and national phones numbers only.

6.2 Communication and computing devices must not be used to dial premium rate numbers (i.e. numbers beginning with the 190x prefix).

6.3 Centacare data accounts and networks must not be used for streaming television and movie content (i.e. a User could use a Centacare device to stream content if the device is connected to their home internet account, but use of data from the Centacare account connected to the device will result in excess data usage).

7. UNACCEPTABLE USE

7.1 Centacare supplied communication and computing devices, data accounts and networks may not be used:
   • for excessive personal use;
   • for commercial activities, such as running any sort of private business, advertising of goods or services or performing work for personal gain or profit;
   • for political activities; such as promoting a political party or movement, or a candidate for political office, or campaigning for or against government decisions;
   • to express views about the workplace, fellow employees, clients, parishioners and/or any entity, wholly or partly of the Roman Catholic Archdiocese of Brisbane;
   • to knowingly misrepresent Centacare;
   • to transmit confidential or personal data outside Centacare unless authorised and/or in accordance with Centacare policies and procedures;
   • to view, create, download, host or transmit (other than for properly authorised and lawful purposes) material that is not of suitable quality and content consistent with a professional Catholic organisation such as pornographic, offensive, obscene, sexually explicit, vulgar or offensive material (i.e. text, language, information, images, video clips, audio recordings, ringtones etc);
   • to view, create, download, host or transmit material which may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious beliefs or political beliefs;
• to retrieve, create, host or transmit any material which is designed to cause annoyance, inconvenience or needless anxiety to others;
• to retrieve, create, host or transmit material which is defamatory;
• for any activity that would infringe intellectual property rights (e.g. unlicensed installation, distribution or copying of copyrighted material);
• creating, using, or distributing copies of software that are not in compliance with the licence agreements for that software;
• for any activity that would compromise the privacy of others;
• for any activity that would intentionally cause disruption to the computer systems, telephones/tablets systems or networks belonging to Centacare or others;
• for any activity that would intentionally waste Centacare’s resources (e.g. employee time and IT resources);
• for any activity that would intentionally compromise the security of Centacare’s IT resources, including the confidentiality and integrity of data and availability of IT resources (e.g. by deliberately or carelessly causing computer virus and malicious software infection);
• for the installation and use of software or hardware tools which could be used to probe, and / or break Centacare IT security controls;
• for the installation and use of software or hardware tools which could be used for the unauthorised monitoring of electronic communications within Centacare or elsewhere;
• for creating or transmitting “junk” or “spam” emails including unsolicited commercial emails, chain-letters or advertisements;
• for disguising the identity of the sender, logging on to the network with someone else’s account, using someone else’s computer to impersonate someone else, sending material anonymously, or allowing an unauthorised User access to the system;
• for any activity that would constitute a criminal offence, give rise to a civil liability or otherwise violate any law.

8. SAFETY WHILE DRIVING

8.1 Use of Centacare supplied communication and computing devices within a vehicle must be in accordance with The Transport Operations (Road Use Management—Road Rules) Regulation 2009 (Qld).

8.2 Staff who are driving any motor vehicle (whether it is stationary, other than parked, or moving) MUST NOT use their Centacare supplied mobile phone/tablet or any other handheld communications device by:
• holding the phones/tablets to, or near, the ear, whether or not engaged in a phone call;
• writing, sending or reading a text message on the phone/tablet;
• turning the phone/tablet on or off; and/or
• operating any other function of the phone/tablet.
9. SECURITY

9.1 Security measures as outlined in the Archdiocesan ICT IT Security Policy will be implemented on all Centacare supplied communication and computing devices including:

- virus protection;
- connection limitation and screen lock processes; and/or
- authentication and password controls.

9.2 Users must ensure their Centacare supplied communication and computing devices is protected at all times. As a minimum all mobile phones/tablets must be protected by the use of a Personal Identification Number (PIN). Other devices and, where it is technically possible, mobile phones/tablets must be password protected.

9.3 Users must take all reasonable steps to prevent damage or loss to their Centacare supplied communication and computing device. This includes, using, where provided, the case or one of similar quality, not leaving it in view in an unattended vehicle and storing it securely when not in use. If it is found that reasonable precautions were not taken the User may be held responsible for any loss or damage to their Centacare supplied communication and computing device.

9.4 A User must immediately report a suspected data breach (a suspicion that personal information has been lost or subjected to unauthorised access, modification, use or disclosure or other misuse) to their line manager in accordance with CCS Policy and Procedure – Incident Reporting and Investigation and Centacare Policy & Procedure – Data Breach.

10. CONFIDENTIALITY & PRIVACY

10.1 In view of the need to observe confidentiality at all times, Users must be vigilant when using their Centacare supplied communication and computing devices in public places in order to avoid unwittingly disclosing personal information of staff, volunteers, contractors or clients and their families.

10.2 Users must be mindful of the risks to confidentiality, and must exercise reasonable caution, when sending text messages which contain any confidential and/or personal information regarding Centacare, its workers, volunteers, contractors, clients and their families.

10.3 Users of Centacare supplied communication and computing devices must not store clients’ personal information in non-Centacare owned or operated applications such as their personal contacts list.

10.4 Communication and computing devices equipped with cameras must not be used inappropriately in the scope of the User’s work for Centacare. In this regard Users:

- must obtain at least verbal consent of all of the persons in the photograph/audio/video recording when using a Centacare supplied communication and computing device to take photographs, audio or video recordings of employees, volunteers, contractors, clients or family members;
- may distribute photographs/audio/video recordings from Centacare supplied communication and computing device:
• when assisting a client to achieve goals and activities in accordance with their Support/Care Plan, (for example when supporting a client to maintain their own Facebook page);
• where the image forms part of the client’s record (for example a photo demonstrating the way in which care should be provided); or
• with the consent of their line manager.

10.5 Users must not post or share a photograph/audio/videorecording photographs, audio or video recordings of employees, volunteers, contractors, clients or a client’s family members to the User’s personal account or share the image/recording on their own social media accounts.

11. LOST OR STOLEN MOBILE PHONES/TABLETS DEVICES

11.1 Users must report the loss or theft of any device to their line manager or After Hours immediately.

11.2 The User must also report the loss or theft in accordance with the Incident Reporting and Investigation Policy and Procedures.

11.3 The line manager must report the incident to the Manager Property and Procurement and:
• for “TRACCS Mobile Devices”, the CIMs Team; and
• for “the computers in houses” project, Archdiocesan Information and Communications Technology.

11.4 On being advised that a Centacare supplied communication and computing device is misplaced, lost or stolen Centacare’s Manager Property and Procurement will wipe the contents of that device immediately, whether or not it is believed to contain personal information.

12. EMPLOYEES LEAVING CCS

12.1 Employees must return their Centacare supplied communication and computing device and any associated equipment (e.g. packaging, case, car kit, battery charger, accessories etc) to the Manager before they leave the employment of Centacare Community Services.

12.2 Employees should remove any personal data before returning the Centacare supplied communication and computing device.

12.3 Users transferring internally within Centacare must ensure that they notify the Manager of both the area they are leaving and the area they are joining to ensure amendments are made to the register of Centacare supplied communication and computing device.

SUPPORTING DOCUMENTS

Related processes and procedures include:
• Centacare Privacy Procedures
• CCS Procedure – Records Management
COMPLIANCE

Deliberate breaches of these Protocols will be dealt with under Centacare’s misconduct provisions, as stated in the Employment Guidelines Code of Conduct.

IMPLEMENTATION

The Directors, Stream Managers and Regional Managers CIMS Team and Archdiocesan Information and Communication Technology are responsible for implementing and monitoring compliance with these Protocols.