Communications Policy

It is the Policy of St Chads Communication Centre Trust to support safe and responsible use of a variety of forms of communication for both the effective operation of the organisation and as a learning tool for clients. The Trust further recognises the need for effective communication both within the organisation and to the wider community/external stakeholders.

This Policy applies to all staff (both paid and voluntary).

The General Manager is responsible for ensuring this Policy is adhered to and any non-compliance with this Policy may be included in the performance and appraisal processes

Guidelines:

1. Public communications are to reflect the current vision and direction of St Chads, are to be of a high standard and be authorised by the General Manger, in communication with the Trust when requested/appropriate, before release. E.g. fliers, brochures, website design, direct campaign letters, prepared press items, information booklets and similar items.
2. Communication to internal stakeholders (e.g family/caregivers) by staff is to be of a professional standard that reflects the messaging authorised by the General Manager
3. St Chads Communication Centre personnel will not use any form of communication to exceed the limits of authority assigned or use any form of communication to conduct business other than that of St Chads Communication Centre
4. Personal use of devices (including calls) will be kept to a minimum
5. St Chads staff will act to protect the security and integrity of the network and stored data
6. The General Manager has the right to monitor access and review all use of technology and internet access and has the authority to carry out an audit at any time
7. The General Manager will have in place a procedure for the collection, use and storage of confidential information related to clients and staff subject to the Privacy Act
8. Usernames and passwords will be kept secure according to best practice guidelines in order to protect St Chad's network infrastructure and information systems from uncontrolled or unauthorised access which may result in intellectual property loss, data destruction or privacy breach
9. The General Manager will ensure staff meetings and appraisals are properly documented to ensure a record is kept. Meetings records are to be available to staff who have been absent to ensure information sharing occurs however it is the responsibility of the absent staff member to access this information
10. Breach of this policy and procedures will constitute gross misconduct and will be dealt with using disciplinary procedures which may include dismissal

Supporting Documents:

- Communications Procedures
- Privacy of Information Policy
- Privacy Act 1993

Document Control Parameters:

- The provisions of this Policy supersede and replace all previous Communications Policies

Policy Review:

- This Policy is to be formally reviewed every second year

Date ratified: Oct 2007	**Date reviewed:** October 2019	**Next review**: October 2021

Communications Procedures

- **Monitoring**
  I. St Chads Communication Centre reserves the right to monitor all external and internal communications where the property of St Chads Communication Centre is used in the communication or is accessed remotely from outside the Centre. This includes the use of portable computers and mobile devices, including mobile phones that may be issued to any person designated by St Chads Communication Centre. Personnel will be advised prior to this occurring
  II. St Chads Communication Centre will take all reasonable steps to ensure that personal communications are not accessed during monitoring, noting however that personal communications are not permitted without the prior approval of the General Manager (see Email/Computer usage guidelines). However St Chads Communication Centre can access personal communication where such communications are partly used to pass information belonging to St Chads Communication Centre or where the nature of the personal communication provides evidence of the breach of this communications policy and procedures
  III. St Chads Communication Centre will not be liable for any breach of privacy should any communications of a personal nature be found and accessed by personnel working for St Chads Community Centre or third parties authorised by St Chads Communication Centre and acting in the course of their work

- **Password protocols**
  I. All network users will be provided with an individual and/or confidential username for their sole use. Usernames will be managed by St Chads. The user is responsible for all activity associated with their username
  II. Users will not share their username and/or password details with any other person. Users will not attempt to discover or change any other person's password. Users will not use their St Chads username or password as a username or password on any non-St Chads systems
  III. Passwords will be robust (at least 7 characters in length and containing at least two numbers, punctuation or special characters). Passwords must be changed every three months or immediately if they have become known to any other party (including personnel designated by St Chads)

- **Internet usage**
  I. The internet will be used responsibly by both staff and clients at all times. Staff using the internet must ensure the use they make is appropriate. This includes but is not limited to:
    - Conducting research and investigation in support of planning service provision and / or

- Communication and information exchange with other colleagues, stakeholders, Government agencies, other organisations as required by business
- Professional development activity

Clients usage needs to be monitored to ensure access meets acceptable standards and is in accordance to any restrictions identified on individual enrolments.

II. The internet will not be used for inappropriate purposes as this may be deemed as 'serious misconduct'. Inappropriate purposes include but are not limited to:
   a. Sexually explicit materials
   b. Violence
   c. Discrimination based on race, sex, religion, nationality, disability, sexual orientation or age
   d. Illegal activities of violation of intellectual property rights
   e. Visiting gambling, gaming, online shopping, "chat rooms" or online dating sites
   f. Uploading or downloading commercial software in violation of copyright

III. The Wifi password is to be kept confidential and not to be given to any unauthorised person

IV. Large files (e.g. videos etc) may not be downloaded at any time by any person without the permission of the General Manager

- **Email/Computer usage guidelines**

I. The email facility within St Chads Communication Centre, (including email addresses), will only be used for communications directly related to work. Personal use is only permitted with the approval of the General Manager and subject to content complying with the Centre's policy and procedure

II. All emails (including replies and forwarded emails) will contain the standard email signature of St Chads Communication Centre which needs to be kept up to date

III. Downloading from any device may only occur if directly related to the work of St Chads Communication Centre. No information is to be uploaded from a St Chads device to any personal or third-party device or to the internet without permission from the General Manager.

IV. Before downloading or uploading occurs or any device is connected to a St Chads device for transferring of information, security risks must be identified and eliminated.

V. No software is to be loaded on any St Chads device without the authorisation of the General Manager.

VI. Portable devices containing confidential information will not be left in any vehicle overnight, and if left in a vehicle for any amount of time they will be out of sight and vehicle doors locked.

VII. St Chads Communication Centre Trust reserves the right to request access to computers or mobile devices (where applicable) at any time to ensure compliance with these guidelines.

VIII. Devices must not be removed from the Centre unless being used to assist in St Chads programmes or for St Chads purposes without the permission of the General Manager.

IX. Clients must not be given access to staff only areas of computer storage

X. Due to the nature of technology systems changing regularly, staff must ensure they are aware of, and follow, current protocols and systems

- **Email etiquette** requires that;
  - All communications will be written in plain, clear language that reflects well on the Centre and meets reasonable professional standards
  - Abusive and / or rude emails or attachments including those that promote the following types of content are unacceptable - Sexually explicit materials, Violence, Discrimination based on sex, religion, nationality, disability, sexual orientation or age, Illegal activities or things that violate intellectual property rights
  - Emails containing confidential or sensitive information will only be sent after checking that the recipient is prepared to receive such information via email. If possible, such emails should be encrypted
  - The Privacy act and applicable St Chads policies will be adhered to at all times.

- **Telephone Use**

I. Local personal calls during personal time will be permissible but should not interfere with the work of St Chads Communication Centre. Toll or International calls of a personal nature will not be permitted unless in an emergency situation and, if practicable, require the permission of the General Manager

II. There will be no restrictions placed on calls for business purposes, where the business of the organisation is being carried out. Such calls will be substantiated and justified on request

III. Telephone voice mail will be used and the message on the voice mail will be correct and up to date. This facility will be used whenever calls are unable to be answered in person

IV. Any confidential and sensitive information discussed by telephone will be done at times and locations when confidentiality can be maintained

V. Mobile phone use whether calling, texting or internet use, can only occur during personal time except in extenuating circumstances and, if practicable, require the permission of the General Manager.

Confidential information storage procedure

All confidential information will be password protected, and backed up off site. Passwords and access is not to be provided to any person without permission from the General Manager.

Date ratified: Oct 2007	**Date reviewed:** October 2019	**Next review**: October 2021