

Otago University Childcare Association (OUCA) Cybersafety, Information, Communication and Technology (CICT) Policy

Rationale:

Information, communication and Technology (ICT) use is an important and financially significant aspect of our environments to be considered with respect. Children, teachers and administration staff have access to and responsibility for data, some of which must be kept safe for privacy reasons. Consideration must also be given to the appropriateness of different uses of ICT within an early childhood environment.

Aims:

1. To establish cybersafe procedures to protect children and adults from access to inappropriate activities/materials.
2. To protect the material stored on ICT from usage for any purpose other than that for which it was collected.
3. To provide guidance to all staff, parents and visitors regarding safe and responsible use of ICT at the OUCA or at any related OUCA activities.
4. To ensure every precaution is taken to secure all OUCA ICT equipment from loss or damage and to provide policies for the updating and quality of equipment.

Definitions:

Cybersafety refers to the safe and responsible operation/use, at any time, on or off the OUCA sites, and by any person, of the centre's internet facilities, network, and associated ICT equipment/devices. This includes but is not limited to computers and laptops, digital cameras, tablets, notebooks, mobile phones and any other equipment which can be used in conjunction with a computer or phone. Also the safe and responsible use by anyone, of privately –owned ICT equipment/devices on an OUCA site or at a OUCA activity.

Appropriate is defined as the usage of ICT as relevant to the business of the OUCA.

Permitted use: OUCA personnel/ECE Students who have signed a cybersafe agreement. Persons contracted to the OUCA to carry out work related to the ICT equipment or programmes with the Director's permission.

Personal use of OUCA ICT equipment by staff during breaks, and outside work hours, is permitted. Accessing inappropriate material is forbidden.

Parents, with the approval of the Director/Head Teacher, have permitted use of OUCA ICT equipment for example a committee member approval for payments..

The OUCA recognizes the importance for some families of having photographs from their children's celebrations, however in order to protect the children, families, and staff of the OUCA, we ask that any photos taken by families at such times are treated with respect and remain off publicly accessible websites such as Facebook etc. Express permission is required at any other time.

While all care and due diligence has been taken in regard to the use of software that is cloud-based information sharing, the OUCA is subject to each providers policies and procedures.

Procedures:

- i. Use agreements will be signed with each person who has legitimate use of the OUCA's ICT equipment.
- ii. Security systems are in operation on all OUCA Computers. Including: updated anti-virus software, updated firewall software and hardware, updated anti-spyware software and the use of passwords.
- iii. The enrolment procedure clearly indicates that by enrolling their child, parents and caregivers agree data involving their child being stored on ICT equipment as part of the learning environment.
- iv. Use of privately owned ICT equipment at the centre are restricted to activities which are appropriate to the learning environment. If using a private camera data must be downloaded to an OUCA google drive account/educa and deleted from the camera card ASAP. In the case of mobile phones, receiving or making private phone calls/texting are acceptable in cases of urgency only, outside of breaktimes therefore they should not be carried when working unless going on an excursion. Mobile phones are not approved for the use of collecting data in the centres.
- v. Any electronic data or files created or modified for the purpose of completing work on behalf of the OUCA on any ICT equipment, regardless of who owns the ICT, are the property of the OUCA.
- vi. Google drive is provided to all staff so that assessment data can be safely stored. No data relating to children, their families or OUCA staff will be stored on memory sticks..
- vii. The Director may conduct an audit of any OUCA computer or other ICT device at any time.
- viii. While using the OUCA internet facilities or ICT equipment/devices or using any privately owned ICT equipment on the premises no person may: initiate access to or have involvement with inappropriate, dangerous or objectionable material or activities, save or distribute such material by copying, storing or printing.
- ix. Accidental access to inappropriate material (can be stopped immediately by covering the screen):
 - a. In the lower range of seriousness e.g.spam –delete
 - b. If more serious e.g. spam containing inappropriate but not illegal material - delete immediately but enter the incident in the ICT Incident Book and block the sender domain from your email inbox.
 - c. If it appears to be illegal material then remove from the view of any child immediately and report the incident to the Director. Centre Management will take such further action as required under this policy.(xii)
- ix. Authorization from the director must be obtained before any attempts to download, install, connect or utilize any unauthorized software or hardware onto or with any OUCA devices/equipment.
- x. When a staff member accesses the internet alongside children the children will be actively supervised.i.e. children will have an adult with them at all times. They may create or send email only under active supervision.
- xi. The principles of confidentiality and privacy extend to accessing or inadvertently viewing information about personnel, or children and their families, which is stored on OUCA equipment.
- xii. Any breach of this policy, which is deemed harmful to the safety of the children at the centre, may constitute serious misconduct.

- xiii As an employee of the OUCA you will have access to confidential information relating to the organization and its families. At no time should this information be referred to in any personal electronic communication.
- All information should be treated as strictly confidential.**
- xiv. OUCA ICT equipment is only permitted to be taken off site for the purpose of adding value to the children's or staff learning experiences and with the permission of a Head Teacher in the case of a camera/tablet, and the Director if a laptop or other equipment.
- xv. Students must sign the OUCA CICT agreement where they wish to take data relating to children away from the premises. The data they take must only be used for the purpose of their teaching studies and must be deleted after their work has been completed.
- xvi. Centre personnel may access the internet for personal use in break times provided this does not interrupt the centre's needs and is of an appropriate nature.
- xvii Annually a minimum of one staff member from each centre will participate in a cybersafety course if available.
- xix Backup procedures. The Association's computer support provider ensures all data not stored 'in the cloud' on the office computer is securely backed-up nightly. Occasional tests will be carried out.
- xx In the case of the presence of family/whanau community member's handheld devices being on premises: no child is allowed to use a personal cellphone for taking photos without the express permission from a staff member.
- xxi Teachers are to take responsibility to be familiar with the terms and conditions of using EDUCA. For information about a child to be posted on EDUCA the consent form must be signed.
- xxii All data about children (and photos) excluding EDUCA, must be deleted after a child leaves the centre unless stored for a specific purpose.

Protocols for Children's use:

- ICT should only be used as a powerful learning and teaching tool, however consideration should be given to children's activity levels, other methods of accessing information and children's overall levels of exposure to ICT.
- When used with a meaningful and strategic approach which is focused on children's learning ICT use with children may be appropriate. Screen time is not recommended for children under 2 years.
-
- Applications are considered by teaching teams for their value as teaching and learning tools. Apps are monitored over a trial period.
- The place of ICT within the children's environment will be supported by agreed pedagogy of each centre.

Date: Oct 2018

Review date: Oct 2019

Budget implications:

Computer Expenses

Professional Development

Policy and other References:

Education Regulations (Early Childhood Education) Reg 46 HS 32

Health and Safety Policy

www.netsafe.org.nz

Otago University Childcare Association

Cybersafety Use Agreement:

I have read the OUCA ICT Policy and agree to follow the procedures listed in the policy:

Name:.....

Signature:

Date:

Facebook Guidelines

The OUCA recognizes that Facebook and other social media are important communication tools for many people. We also acknowledge it is important to be aware of how to keep yourself and your relationships safe by managing your information appropriately.

Here are some guidelines to support you when you are using Facebook:

Firstly always use your common sense and think about the impact on other people and yourself now and in the future.

- Assume you are communicating in a public space.

When you are communicating on Facebook, remember a range of people could have access to the information: centre parents, colleagues, friends and your employer.

- Think to yourself, would I feel comfortable saying this in person? If you want to have a private conversation use the privacy settings to protect yourself. If you want to talk about something that is confidential or sensitive, face-to-face talk would be more appropriate.
- It is not OK to use Facebook to put people down or to make disparaging remarks about others, this is particularly true of your work place and the people in it.
- Never discuss private or confidential information on Facebook even in general terms. People are very good at reading between the lines.

You are not obliged to accept all friend requests. If you feel uncomfortable rejecting a request you can adjust your privacy settings and choose the information they see about you.

- Using your privacy settings is a key to protecting yourself and others.

Think carefully about whom you will become friends with.

- How will you feel if a parent complains about your centre/colleagues on Facebook?
- What would you do with that information?

It is expected that photographs from work functions will not be uploaded. Always gain the persons permission before uploading photographs or tagging another person.

- If you want to share photos, do it using the private setting.

Take time to become familiar with and understand the privacy options on Facebook. Make sure you know how to control who can see the different parts of your profile.

Remember to use your common sense. If you feel uncomfortable about it don't put it on Facebook, it could be there forever!