**Child Safety in Online Environments:**

These guidelines are for Society programs and services where we provide internet / computer access to children and young people and includes all personnel in those programs.

# Physical Locations of Devices

# Where possible, computers and other devices should be used in an open environment where program or service personnel can supervise the activity.

# Accessing Wi Fi

Where WiFi services are used, parental controls must be set to an age-appropriate level, to restrict adult and inappropriate content.

## Internet usage

A web filter tool must be used on all Society devices provided to children and young people. To determine which categories to filter, follow the NSW Department of Education standards <https://policies.education.nsw.gov.au/policy-library/policies/pd-2020-0471>. Although the following is not an exhaustive list, web filters on the devices will exclude the following:

* Obscene digital material or pornography
* Jokes, video clips, images, text, or other displays which contain material or words that negatively reflect on a particular race, gender, religion, colour, national origin, disability, sexual preference, marital status, or status as a parent or carer
* Shopping
* Mature adult material
* Websites that support illegal or unethical activities
* Anything that attempts to compromise the security of a device.

*YouTube* access should be locked on the devices. Note that the NSW Department of Education blocks *YouTube* access to students until Years 11 & 12 due to unfiltered and inappropriate content. *ClickView* and *Vimeo* – have educational content devised by Educators and IT Professionals - are suggested as alternatives by the NSW Department of Education. YouTube Kids is an appropriate alternative.

## Briefing

Children and young people accessing Society devices should be briefed inappropriate online behaviour. Briefs should be age-appropriate and should include:-

* Acceptable use of the device
* Appropriate interactions with others / bullying
* The importance of not sharing personal details, location etc
* Where to go if they need assistance or to report an issue
* Appropriate sites and content
* Consequences for breaches of the rules or guidelines

## Social media usage

All social media activity must comply with and adhere to the Society Code of Conduct, the Social Media Policy, the Society Privacy Policy and the Society Safeguarding Children and Young People Policy.

## Camera usage

Access to cameras should be locked unless a project specifically requires it.

## Storage of data

Devices provided to children and young people in our programs or services should not be used to store data or personal information of any kind.

## Security

Devices must not be left unattended in public places. After usage, all devices must be stored securely.

Devices are not to be taken home by children, young people or personnel.

**Passwords**

Passwords should be chosen and managed by the Administrator, following Society IT process. Passwords should only be provided on a need to know basis. Administrator passwords must not be shared.

## Incidents and breaches

An incident includes both:

* security incidents - where it is suspected or confirmed there is a threat to Society’s Information Services; and/or
* an incident which is suspected or confirmed to compromise safety for a child or young person (in any way).

## Control Exceptions

All exemptions request must be reviewed and assessed for both IT security and child safety concerns and approved by the Director or Regional Director.