ATTACHMENT 1
Procedures for use of ICT at the service

EMAIL USAGE

- Content of emails and email addresses must always be checked before sending.
- When sending emails to multiple recipients, care should be taken to avoid the inappropriate disclosure of email addresses to a whole group of recipients; blind copying (BCC) should be used where appropriate.
- Always include a subject description in the subject line.
- Always include a disclaimer (refer to *Definitions*) which is common to all users, on emails to limit liability.
- Be cautious about opening files or launching programs that have been received as an attachment via email from the email itself. Instead, save an attachment to disk and scan with anti-virus software before opening, and keep an eye out for unusual filenames.
- Never open emails if unsure of the sender.
- Check email accounts on a regular basis and forward relevant emails to the Approved Provider-Shine Bright EYM, relevant staff or appropriate PAG members/.(e.g. Fundraising)
- Remove correspondence that is no longer required from the computer regularly.
- Respond to emails as soon as is practicable.

UNACCEPTABLE/INAPPROPRIATE USE OF ICT FACILITIES

Users of the ICT facilities (and in particular, the internet, email and social media) provided by Shine Bright EYM - must not:

- create or exchange messages that are offensive, harassing, obscene or threatening
- create, copy, transmit or retransmit chain emails (refer to *Definitions*), spam (refer to *Definitions*) or other unauthorised mass communication
- use the ICT facilities as a platform to gain unauthorised access to other systems
- carry out activities that are illegal, inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules/discriminates against others on the basis of race, nationality, creed, religion, ability/disability, gender or sexual orientation
- use the ICT facilities to access, download, create, store or distribute illegal, offensive, obscene or objectionable material (including pornography and sexually explicit material). It will not be a defence to claim that the recipient was a consenting adult
- use the ICT facilities to make any personal communication that could suggest that such communication was made in that person's official capacity as an employee or volunteer of Shine Bright EYM
- conduct any outside business or engage in activities related to employment with another organisation
- play games that are not relevant to children's learning
- assist any election campaign or lobby any government organisation
- exchange any confidential or sensitive information held by Shine Bright unless authorised as part of their duties
- publish the service's email address on a 'private' business card
- harass, slander, intimidate, embarrass, defame, vilify, seek to offend or make threats against another person or group of people
- breach copyright laws through making copies of, or transmitting, material or commercial software.

INFORMATION STORED ON COMPUTERS

- Computer records containing personal, sensitive and/or health information, or photographs of children must be stored securely so that privacy and confidentiality is maintained. This information

must not be removed from the service without authorisation as security of the information could be at risk (refer to *Privacy and Confidentiality Policy*).

- Computer records containing personal, sensitive and/or health information, or photographs of children may need to be removed from the service from time-to-time for various reasons, including for:
  - excursions and service events (refer to *Excursions and Service Events Policy*)

  In such circumstances, services must ensure that the information is transported, handled and stored securely so that privacy and confidentiality is maintained at all times.
- Computer users are not to view or interfere with other users' files or directories, knowingly obtain unauthorised access to information or damage, delete, insert or otherwise alter data without permission.
- Ensure all material stored on an endpoint data storage device is also stored on a backup drive, and that both device and drive are kept in a secured locked away location in a locked office

BREACHES OF THIS POLICY

- Individuals who use ICT at the service for unlawful purposes may be liable to criminal or civil legal action. This could result in serious consequences, such as a fine, damages and/or costs being awarded against the individual, or imprisonment. The Approved Provider- Shine Bright EYM will not defend or support any individual using the service's ICT facilities for an unlawful purpose.
- The service may block access to internet sites where inappropriate use is identified.
- Employees who fail to adhere to this policy may be liable to counselling, disciplinary action or dismissal.
- Management, staff, volunteers and students who fail to adhere to this policy may have their access to the service's ICT facilities restricted/denied.