2.17 Cyber-Bullying

Policy Statement

We acknowledge we have a responsibility and duty of care to ensure that the rights of employees, volunteers, children and families to be physically, emotionally and psychologically safe whilst participating in on-line activities associated with the service, are protected. This responsibility may extend beyond service on-line activities, where such inappropriate behaviour, impacting harmfully upon employees, volunteers, children and families, becomes known.

We aim to articulate the rights and responsibilities of employees, volunteers, children and families associated with the service with regards to cyber-bullying.

Definitions

'ICT': information and communication technology.
'Cyber-bullying': involves the use of information and communication technologies to support deliberate, repeated and hostile behaviour by an individual or group that is intended to harm others. Cyber-bullying might occur over the Internet, in instant messaging (IM), chat rooms, social networking sites, blogs, gaming sites, over the phone by SMS or MMS, by email or via other technologies.
While cyber-bullying is similar to real life bullying, it also differs in the following ways:

- It is invasive, can occur 24/7 with a person being targeted at home, work or anywhere;
- It can involve harmful material being widely and rapidly disseminated to a large audience. For example, rumours and images can be posted on public forums or sent to many people at the 'press of a button';
- It can provide the bully with a sense of anonymity and distance from the victim so there is a lack of immediate feedback or consequences.

'E-crime': occurs when a computer or other electronic communication device (e.g. mobile phone) is used to commit an offence, is targeted in an offence, or acts as a storage device to an offence.

Procedures

Service Responsibilities

- We will ensure families are aware of the cyber-safety practices and encourage any employee, volunteer, children or families who are accessing ICT equipment or devices at the service.
- The Coordinator will ensure all information posted to electronic media (e.g. internet web pages, news groups, web-based forums, Facebook) conforms to acceptable standards of respectable on-line behaviour. This may include ensuring that confidential information is not accessible on publicly available websites and that images posted don't include any identifying images of the children without prior written permission from their parent/guardian.
- The Service will ensure all educators are provided with training and support in managing instances of cyber-bullying when children are accessing ICT equipment and devices.

- Strategies and guidelines will be developed, in collaboration with the children, for using the ICT equipment and devices respectfully whilst in attendance at the service. This may include the development of 'user agreements', in collaboration with educators, children and families. Children's personal mobile devices are not permitted to be used whilst at the service, unless it is an emergency and the Coordinator (or Nominated Supervisor) has provided authorisation.
- In consultation with management, if there is suspicion that an e-crime has been committed; the Coordinator will report it to the police. Where there is further reasonable suspicion that evidence of a crime, such as an assault, is contained on a mobile phone or other electronic device, the device will be confiscated and handed to the investigating police officer. The electronic device should not be tampered with.
- We may also be required to complete a 'Notification of Serious Incident' form and forward it to the Regulatory Authority.

Educator Responsibilities

Educators will:

- Ensure their own practices role model appropriate safety measures when researching information, either individually or with the children.
- Ensure children are only able to access the internet at the service through authorised computers that have been fitted with appropriate security and filtering software
- Will encourage children to follow service guidelines and strategies for dealing with instances of cyber-bullying, as detailed in the "user agreement" that your child has with Tewantin State School.
- Encourage children's safe use of the internet, through implementing the following cyber-safe practices whilst participating in service related activities:
- Never posting personal information such as address or telephone number online;
- Never posting photos of themselves (such as 'selfies') online;
- Not responding to any messages that are mean or in any way make them feel uncomfortable;
- Not sending any messages that may be mean or make another person feel uncomfortable;
- Never agreeing to meet any person they have met online;
- Never giving their internet user name or passwords to another person (even best friends);
- Checking with an educator before downloading or installing any software or games;
- Informing an educator if they access information that makes them feel uncomfortable.

Family Responsibilities

Inform the Coordinator of any concerns you may have in regard to cyber-safety and your child, whether it is happening at the service or not.

Please be aware of your child's access to data on devices, whether securely connected through the service or accessible on their own device. Lastly, encourage your child to share information, including social networking sites (Facebook) with you as a 'friend' to monitor their safety online.

References

Education and Care Services National Law Act, 2010 and Regulations 2011
Family and Child Commission Act 2014
Child Protection Act 1999 and Regulations 2000
Work Health and Safety Act 2011
Duty of Care
Relevant Policies: Safety and Wellbeing of Children, Protecting Children from Harm, Anti-Bullying, Children's Property and Belongings, Promoting Protective Behaviours, Educational Program Planning, Provision of Resources and Equipment, Communication with Families, Risk Management and Compliance, Information and Technology.