E-Safety, Networking and Mobile Phone Policy

Principle

E-safety concerns safeguarding children, young people and staff in the digital world. Technology is an important part of everyday life and so E-safety focuses on learning to understand and use new technology in a positive and safe way. The purpose of this policy therefore is to help support and protect children and staff when using technology on the setting.

Policy

This policy applies to all employees, volunteers, visitors and members of the public who use our premises. This policy covers internet, email and all electronic communications via computers, laptops, mobile phones, iPhones and other wireless technology.

Procedure

All staff members are responsible for the following:

- Understanding the risks and responsibilities which are part of the 'Duty of Care' that applies to everyone working with children.
- Understanding the significance of E-safety which highlights the importance of safeguarding children.
- Reporting any knowledge or suspicion of behaviour that contravenes this policy.
- Being aware of the potential risks of using social networking sites, e.g. Facebook and the importance of considering the material they post and how posting unsuitable material may affect their professional status.
- Protecting themselves from legal challenge and ensuring that they work within the boundaries of professional behaviour.
- Ensuring they do not create any unnecessary business risk to Rainbow Stop Playgroup by the misuse of email and internet systems.
- Complying with current legislation.
- Using the internet in an acceptable way.

In particular the following behaviour and use of systems are deemed unacceptable:

- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material.
- Sending, forwarding, distributing or retaining email or text messages that contain language or images that are abusive, aggressive, obscene or offensive.
- Making any improper or discriminatory reference to a person's race, colour, religion or belief system, sex, age, national origin, sexual orientation, disabilities or physique and forwarding or distributing any material which does so.

- Publishing defamatory and/or knowingly false materials about Rainbow Stop Playgroup.
- Using work email systems to set up or send chain letters, viral emails or spam.
- Using the internet for personal purposes during work time.
- Using the computer to participate in any form of fraud, theft or software or music piracy.
- Failing to take due care to make sure confidential and/or personal information goes to the correct recipient.
- When representing Rainbow Stop Playgroup, broadcasting personal views n social, political, religious or other non-business related matters.
- Undertaking deliberate activities that waste staff effort o networked resources.
- Sending an unauthorised email on behalf of an individual inside or outside Rainbow Stop Playgroup without their knowledge or consent.

Specific arrangements for the use of mobile phones are as follows:

- Staff personal mobile phones must be switched off and not used during the session.
- Mobile phones should not be carried by staff and should be stored in a secure place.
- The setting has a telephone for incoming and outgoing calls – this number may be given by staff as an emergency contact number for incoming calls only.
- If a member of staff is expecting an emergency or important call, then their personal mobile phone may be switched on but must not be kept on their person. Permission may be sought from the leader who will agree and determine a suitable area where the phone is accessible should the need arise.
- During group outings nominated staff will have access to the settings mobile phone, which is for emergencies only.

The leader is responsible for:

- Ensuring that mobile phones even if turned off are not carried by staff during the relevant policies.
- Ensuring staff are aware of and understand this policy and how it links to other relevant policies.
- Putting relevant systems in place to ensure protection of information and appropriate access to the internet, e.g. passwords on computers, limited access to certain websites.
- Monitoring the policy to ensure staff are complying with it, this includes the right to access emails, images and internet sites visited, where there is suspicion of improper use.

- Dealing with breaches of the policy and ensuring that the highest standards of practice are maintained.

Breach of Policy:

- All employees should be aware that any failure to comply with this policy will be taken seriously and may be dealt with in accordance with Rainbow Stop Playgroup's Policy and Procedures.
- If an employee is found to have breached this policy, they will face a disciplinary penalty ranging from a verbal warning to a dismissal.
- Where criminal offence is suspected, the matter will be referred to the PSNI.

This Policy was reviewed on: 27th February 2015