Policy on E-Safety,Mobile Phones,Social Networking

Purpose

E-Safety concerns safeguarding children, young people and staff in the 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 in our setting.

Scope

The policy applies to all employees, volunteers, visitors and members of the public who may enter our setting..

Responsibilities

All staff members are responsible for the following:

- Understanding the risk and responsibility that is 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 and keeping them safe, which is of paramount importance.
- Reporting any knowledge of 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 materials they post and how publishing unsuitable materials may affect their professional status.
- Protecting themselves from legal challenge and ensuring that they work within the boundaries of professional behaviour.

- Ensuring that no unnecessary professional risk occurs to Holy Trinity Pre-School/After School Club by the misuse of the internet or email systems.
- Complying with current legislation.
- Using the internet in an acceptable way.

In particular, the following is deemed unacceptable use of behaviour of staff:

- 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.
- Using the internet to send offensive or harassing material to others.
- 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 not forwarding or distributing any material which does so.
- Publishing defamatory and/or knowingly false materials about Holy Trinity Pre-School/After School.
- Publishing any information relating to other staff or children without the express permission of the individual or in the case of children, their parents.
- Using work e-mail systems to set up or send chain letters, viral emails or spam.
- Using the computer for personal purposes during work time.
- Using the computer to participate in 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.
- Broadcasting personal views on social, political, religious or other non-business related matters.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Sending an unauthorised e-mail on behalf of an individual inside or outside Holy Trinity without their knowledge or consent.
- Making reference to any aspect of work such as referring to other staff/pupils/parents or including any photographs of any of the above within a social media setting.

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; the setting has telephone/mobile phone for incoming and outgoing calls - this number may be given by staff as a work/emergency contact number for incoming calls only.
- If a member of staff is expecting an emergency or important call, their personal mobile phone may be switched on but must not be kept on their person. Permission may be sought from the supervisor who will agree a suitable area or place where the phone is accessible should the need arise.
- During outings nominated staff will have access to the setting nominated mobile phone, which is used for emergency purposes only.

Good Practice

- Ensuring that staff are aware of and understand this policy and how it links to other relevant policies.
- Putting relevant systems in place to ensure the protection of information and appropriate access to the internet, e.g passwords on computers, limited access to certain websites.
- Monitoring the policy to ensure that staff are complying with it; this includes the right of the Manager/Principal to access e-mails, images and internet sites visited, where there is a suspicion of improper use.
- Dealing with breaches of the policy and ensuring that the highest standards of practice are maintained.

Other Key Policies

This policy is relevant to a number of other policies and should be read alongside them:

- Child Protection Policy
- Confidentiality Policy
- Disciplinary Policy

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 After School Disciplinary Policy and Procedures. If an employee is found to have breached the policy, they will face disciplinary action ranging from a verbal warning to a dismissal. Where a criminal offence is suspected, the matter will be referred to the PSNI.