

SOCIAL NETWORKING POLICY

1. Introduction

- 1.1 The Community Playgroup recognises that many employees use the internet for personal purposes and that many employees participate in social networking on websites such as Facebook, Twitter, MySpace, Bebo and Friendster etc.
- 1.2 The purpose of this policy is to outline the responsibilities of employees using social networking websites.

2. Personal conduct

- 2.1 The Business respects an employee's right to a private life. However, The Community Playgroups must also ensure that confidentiality and its reputation are protected. It therefore requires employees using social networking websites to:
 - 2.1.1 Ensure that they do not conduct themselves in a way that is detrimental to The Community Playgroups;
 - 2.1.2 Take care not to allow their interaction on these websites to damage working relationships between members of staff and clients of the Business.
 - 2.1.3 Report any concerns they have to their Manager about information disclosed on social networking/internet sites.
 - 2.1.4 Employees should not accept friend requests from parents on social networking websites, nor should they request to be friends with a parent. In the situation where employees are already friends on a social networking website with a parent prior to their child starting at playgroup, the Business understands that employees will remain friends with that parent, however, in no circumstances should playgroup, the children, the staff or any other Business matters be discussed or commented on over social networking websites.
 - 2.1.5 Under no circumstances should social networking websites be accessed from the Business's internet devices or during your normal working hours, unless it is during your break time and in an area which is inaccessible to the children.

3. Security and identity theft

- 3.1 Employees should be aware that social networking websites are a public forum. Employees should not assume that their entries on any website will remain private.

- 3.2 Employees should never send abusive or defamatory messages. Comments made may be deemed slander that could lead to prosecution.
- 3.3 Employees must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords.
- 3.4 In addition, employees should also protect children and parents using our services and should therefore:
 - 3.4.1 Ensure that no information is made available that could provide a person with unauthorised access to the Business and/or any confidential information; and
 - 3.4.2 Refrain from recording any confidential information regarding the Business on any social networking websites.
 - 3.4.3 Ensure that no pictures are added that include images of children from the playgroup.
 - 3.4.4 Never disclose any details whatsoever of staff, parents or children.
 - 3.4.5 Never disclose details of existing or potential customers.
 - 3.4.6 Report anything to their Manager where the above has been breached by any other person, including ex-employees.
- 3.5 Please be aware that any breach of this is policy could result in disciplinary action including dismissal.

4. Recruitment

- 4.1 At no stage during the recruitment process will the managers or leaders conduct searches on prospective employees on social networking websites. This is in line with the Business's equal opportunity policy.