An e-Safety and Social Media Policy and Procedure For BS3 Community Development Early Years Nurseries.

Who is the toolkit for? The toolkit is designed to be used by BS3 Community Development Nurseries providing services for the early years age group (birth –5 years); however as good practice it can be applied to any part of the organisation working with children. The toolkit will aim to provide guidance on best practice for managing the risks associated with e-safety through policies and procedures and includes exemplars. If settings are using social networking sites e.g. Facebook and Twitter to promote their business, the registered person / safeguarding designated officer for the setting needs to be aware of and adhere to the safeguarding protocols associated with these sites and work in line with the Communications Manager.

It should be viewed as essential that parents and carers are fully involved in promoting online safety in the setting and at home. It will be beneficial to regularly consult with and discuss online safety issues with parents and carers with an aim to encourage a better understanding of the benefits and risks associated with ICT. ICT is considered an essential life skill and will significantly contribute to children's enjoyment of learning and their development. In early years it is not normally expected that children would be accessing social media, however practitioners should be aware of age restrictions for each social media site used. **'e-safety** could be described as a settings ability to protect and educate children and staff in their use of information communication technology (ICT) with

appropriate, effective systems in place to intervene and support with any incident (Ofsted document Inspecting e-safety reference number 120196, April 2014). Legislation Settings are advised to risk assess social media tools to comply with The Health & Safety at Work Act 1974, The Children Act 1989, The Childcare Act 2006, The Management of Health and Safety at Work Regulations 1999 and The Computer Misuse Act 1990 which clarify that all settings have a duty of care to ensure the safety and wellbeing of children and early years staff. The Statutory Framework for the Early Years Foundation Stage pg.17, 3.6 states; 'training made available by the provider must enable staff to identify signs of possible abuse and neglect at the earliest opportunity and to respond in a timely and appropriate way. Providers must train all staff to understand their safeguarding policy and procedures which should include inappropriate behaviour displayed by other members of staff which includes the inappropriate sharing of images'.

2.0 e-Safety Policy

2.1 Aim

To ensure early years practitioners have a clear and agreed understanding of the benefits and risks of e-safety. It will provide advice on acceptable use and effective control measures to enable individuals to use ICT resources in a safe online environment.

- Safeguarding children is everyone's responsibility, it is of paramount importance to always ensure the safety and wellbeing of children and this includes their online safety.

- The registered person will have the overall legal, personal, and moral responsibility to ensure that online safety is effectively considered.

- The designated persons for safeguarding is to be responsible for online safety alongside the administrator for social media, and will manage the implementation, monitoring and reviewing of the e-safety policy.

- To minimise any risks all staff should have effective training on e-safety.

- Creating a safer online environment will be on-going, so clear monitoring, evaluation and review of procedures are essential.

- Early years Assistants and practitioners should support children's emerging understanding of e-safety by providing a range of resources to support their learning including cameras, iPad, tablets, computers, and any other devices.

- Practitioners should be committed to acknowledge and assess risks to create a balanced approach. Relevant documentation such as incident logs (Appendix 5) and written risk assessments must be completed in accordance with our policies.

2.2 BS3 Community Development's **Social Media Policy and Procedure**

Social media tools can provide excellent opportunities for teaching and learning; however such sites can have risks and can never be 100% safe. These risks can be minimised by having an embedded e-safety policy and individuals should consider having separate personal and business on-line communication tools.

2.3 Administration & Monitoring

Practitioners must be aware of their personal and professional conduct when using social media. Practitioners using social media should consider what information is published to ensure confidentiality GDPR- is always observed and the setting is not brought into

disrepute. Content can be easily shared online and circulated far and wide without consent or knowledge, possibly resulting in disciplinary, civil, or criminal consequences.

At BS3 Community Development our aim is to Promote positive use of new and emerging technologies, we wish to Involve parents and carers in developing and reviewing our daily practice and we must take into consideration Ethical Considerations by communicating frequently with our customers. As a communication tool user staff member should consider the potential associated dangers of posting images, photographs and information on social networking sites. Key safety concerns include:

- Children being easily identified by their image posing a risk of inappropriate contact by individuals (children's names must not be displayed alongside their images)
- Images being altered and distorted
- Images being used inappropriately causing stress and anxiety

All individuals regardless of age should have a right to participate in the decision making of how information is used and published. The views of children must be considered to comply with 'United Nations Convention on the Rights of the Child':

- Article 3: Best interests of the child
- Article 12: Respect for the views of the child
- Article 13: Freedom of expression
- Article 16: Right to privacy

3.0 Acceptable Use Policy (AUP)

Aim AUP gives users a clear understanding of what staff employed by BS3 Community Development and volunteering can and cannot do, how their use of Social media will be monitored and the sanctions for misuse. AUP will apply to all individuals, with the registered person having overall responsibility for ensuring that online safety is implemented as part of everyday safeguarding practice. Clear, robust policies and procedures, including allegations of misuse, should be available.

AUP should outline the responsibilities of all individuals who have access to and use of ICT systems and ensure that everyone has a clear understanding of what constitutes misuse and the sanctions that may be applied. ACTION- Individuals will be asked to sign the back of the policy and date it.

Staff must be aware that any inappropriate behaviour/actions will be taken seriously and in the event of an allegation of misuse, the designated e-safety administrator (Deputy Administrator) must inform the setting safeguarding officer who will contact the police if it is a criminal matter or First Response if it is a safeguarding or welfare concern.

Childcare practitioners should not have personal communication, including on social network sites, with the children, parents, and carers with whom they act in a professional capacity. There may be occasions when the practitioner and the adults in the family are friends prior to the child coming into the setting. Or employee babysits for a parent or carer. This information should be shared with the manager and documented as a conflict of interest. The Room leads will inform the Head of Early Education and Childcare.

As part of the registration process, Parents need to be consulted and must provide written agreement for their children to access online resources which will also be monitored by a supervising adult (Appendix 2: eSafety Parental Permission Form attached)

Employee Agreement:

Any devices equipped with internet access should be considered subject to the same risks as any other form of technology.

All personal mobile phones need to stored in a locked locker not in the rooms with children.

All devises with cameras are forbidden in any rooms. This includes Camera watches.

Strong passwords (combination of numbers, symbols and lower/upper case letters) are essential, must be kept secure and be regularly updated.

I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.

I will only use chat and social networking sites in accordance with the setting's policies.

I will not engage in any online activities that may compromise my professional responsibilities.

I will only communicate with parents, carers and other professionals using official systems. Any such communication must be professional in tone and manner.

If I fail to comply with this Agreement, I could be subject to disciplinary action.

I have read and understood the above and agree to use BS3 Community Development systems, both in and out of the setting, and my own devices, within these guidelines.

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/

Practitioner's name: _____ Signature: _____ Date: ___

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____ Date: ___/___/__

Practitioner's name: _____ Signature: _____
Date: ___/___/__

Practitioner's name: _____ Signature: _____
Date: ___/___/__