Early Education & Childcare

Online Safety and Social Media policy

Aims:

-To ensure that BS3 Community Development are compliant **to comply with national guidance and legislation. This includes:**
Working Together to Safeguard Children which outlines what individuals, organisations and agencies must do to protect children from harm and promote their welfare.
Keeping Children Safe in Education which is statutory guidance for all staff working in Early Years, Schools and Colleges which outlines their responsibilities to provide a safe environment in which children can learn. This guidance was last updated in June 2023 and applies from 1 September 2023.
Early Years Foundation Stage Statutory Framework which outlines the standards that school and childcare providers must meet for the learning, development and care of children from birth to 5 years old. This Early Years Foundation Stage (EYFS) framework is mandatory for all group and school-based early years providers in England from 4 January 2024.
-To ensure BS3 Community Development have a data processor that liaises with the safeguarding designated officer (Head of Early Education and Childcare, Kelly Murphy) and the Head of Operations Manager (Becca McDougall) for the setting and adhere to the safeguarding protocols associated with online safety and social media work.

In early years it is not normally expected that children would be accessing social media, especially when attending our settings. 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. Social media tools can provide 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 online policy and individuals should consider having separate personal and business on-line communication tools. BS3 Community Development provide all staff with access to a professional email account to use for work related business including communication with parents and carers. This allows for content to be monitored and protects staff from allegations or inappropriate contact with children and their families. Any emails from the room must copy in our Family Services department email address. All

emails should be professional in tone and checked carefully before sending, just as an official letter would be.

The Statutory Framework for the Early Years Foundation Stage 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'.

To ensure early years practitioners have a clear and agreed understanding of the benefits and risks of online safety. We provide acceptable use and effective control measures to enable individuals to use ICT resources in a safe online environment. This includes:

- 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 are to be responsible for online safety alongside the administrator for social media, and will manage the implementation, monitoring and reviewing of the online safety policy.

- To minimise any risks, all staff have effective training on e-safety, this included within our annual Child Protection training.

- 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 develop their learning including cameras, iPad, tablets, computers, and any other devices.

Administration & Monitoring

Famly is used as our online journal system and allows staff to track and share a child's learning journey online with parents and carers, usually in the form of text and photographs. This has considerable benefits including improved levels of communication with families. Personal staff mobile phones or devices (e.g. iPad or iPhone) should not be used for any apps which record and store children's personal details, attainment or photographs. Only setting-issued devices may be used for such activities. Devices with sensitive information should be secularly locked and stored away after each session.

Staff should only take information offsite when authorised and necessary, on occasions when this is necessary staff should ensure the that the information is

protected. Staff should take appropriate action to reduce the risk of theft. Staff should ensure they have signed out of any IT equipment they have.

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 and GDPR (General Data Protection Regulation), Staff members need to ensure that they are professional at all times and that the setting is not brought into disrepute and remember that 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

Staff employed by or who are volunteering in BS3 Community Development must know what they can and cannot do whilst working here how their use of social media will be monitored and the sanctions for misuse. An Accessible User Policy (AUP) will apply to all individuals, with the Head of Operations 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. Individuals will be asked to sign the back of the policy and date it to demonstrate that their responsibilities have been communicated to them and that they agree to adhere to the policy.

Staff must be aware that any inappropriate behaviour/actions will be taken seriously and in the event of an allegation of misuse, the designated Head of Operations must inform the setting safeguarding officer (DSL) 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 and kept in the employee files. 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)

IT safety and data protection

As an Early Years provider, we must have strong IT infrastructure and data protection practices. We ensure that BS3 Community Development:

- uses a firewall and robust antivirus software
- uses a recognised internet service provider
- uses an encrypted and password protected Wi-Fi network
- actively monitors and filters any inappropriate websites or content
- manages data in compliance with the Data Protection Act 2018.

The Information Commissioner's Office (ICO) provides advice on data protection for organisations across the UK (ICO, n.d.), whilst the Department for Education (DfE) provides further, specific guidance for schools in England (DfE, 2023a).

Filtering and monitoring

We have a rolling contract with Sharp IT, have effective filtering and monitoring systems in place and Our Head of Operations and IT processor Becca McDougall ensures that our systems safeguard children from harmful online material and provide a safe environment for learning. Filtering restricts access to online content, while monitoring allows user activity to be reviewed. In England, the Department for Education's (DfE's) filtering and monitoring standards for schools and colleges provides further detail about the systems schools should have in place, including:

- a filtering system that blocks internet access to inappropriate and harmful content. The system should not excessively restrict the day-to-day needs of the organisation or stop students learning how to recognise risk themselves
- an effective monitoring strategy that allows incidents to be quickly recognised and recorded
- clearly identified roles and responsibilities for staff and third parties. This should include assigning a member of the senior leadership team and a trustee to be responsible for ensuring the standards are met.
- regular reviews (at BS3 Community we do every 6 months) of the filtering and monitoring provision to check that systems are working as expected.

- BS3 Community Development takes data security and privacy very seriously because we know that confidentiality and the protection of information is a fundamental feature of our relationship with our service users. When we use your personal data, we are required to do so in accordance with the General Data Protection Regulation (GDPR). We are responsible as 'controller' of your personal data for the purposes of the GDPR. We will use your personal data in accordance with your engagement with us and your instructions, the GDPR, other relevant UK legislation and our professional duty of confidentiality. You can read our full policy here: https://bs3community.org.uk/data-protection-policy-2/

Employee Agreement:

I understand that:

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 be stored in a locked locker, and 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: _____

Related documentation:

- Child Protection and Safeguarding Policy
- Equal Opportunities Policy
- Whistle Blowing
- Escalation Policy
- Positive Handling Policy
- Mobile Phone and Camera Policy