Online Safety Policy

Online safety is recognised as part of the Bright Beginnings Childcare Centre's safeguarding responsibilities.

The Designated Safeguarding Lead (DSL) takes lead responsibility for online safety concerns.

Online safety concerns are reported to the DSL, recorded and actioned. Children are enabled (at a level appropriate to their age and ability) to share online concerns.

To raise awareness of online safety concerns Bright Beginnings will consider the following regarding online safety concerns:

Our policies cover:

- Safe and appropriate use of personal devices, wearable technology, mobile phones and cameras.
- Acceptable and appropriate use of technology within the setting
- Expectations regarding professional boundaries/behaviour of staff, including communication via social media
- Policies and procedures are easily accessible to staff and parents/carers, for example, published on the setting's website.
- Staff and parents/carers are consulted and actively involved, as far as possible in the development of policies
- Policies have been reviewed and approved by the management team
- The Capture Policy and Procedure is shared with staff when they commence employment at Bright Beginnings. Staff will be made aware that failure to adhere to the usage policy may result in disciplinary action.

DSL and Management are aware of how and why technology is used within the setting by staff and children.

The types and numbers of devices are monitored by the General Manager. If these devices are connected to the internet this must be accessed via the secure network provided by The University of Leeds.

Appropriate filtering and monitoring is in place and advice is available from the UK Safer Internet Centre.

Access to setting's devices is managed and monitored in line with the University of Leeds IT policies and procedures .

Setting's devices are kept securely and in line with data protection requirements. Practitioners will not be permitted to take the devices home. The devices are stored in area cupboards which are secured by a key code lock at the end of the Centre day.

Physical safety of users has been considered e.g. posture of children/staff when using devices.

Personal data is managed securely online, in accordance with the statutory requirements of the General Data Protection Regulations (GDPR) and Data Protection legislation.

Managers will ensure that all staff:

- Are provided with quality and up-to-date online safety training provided by The University of Leeds on receipt of their personal University login details.
- Appropriately supervise children whenever they are using devices and ensure that children receive age appropriate, progressive and embedded online safety education throughout the curriculum and use age appropriate tools and resources.

Online Safety Policy

- Check apps, websites and tools prior to using them with children, this should include checking the results of searches
- Use age appropriate apps, websites and online tools with children
- Model safe practice when using technology with children
- Ensure data is shared online in accordance with the data protection responsibilities
- Know how to report a problem and when to escalate a concern.
- Are aware that under no circumstances should any member of staff, either at work or in any other place, make, deliberately download, possess, or distribute material they know to be illegal, for example child sexual abuse material.
- Are aware that no matter what privacy settings are used, anything posted online can become public and permanent and could be misinterpreted and/or used without their knowledge or consent.

Managing online relationships

- You should not add parents of children at your setting as friends online; this can blur professional relationships and put you at risk of allegations. If there is a pre-existing relationship or situation which means this is not achievable, you should discuss this with the DSL at your setting and/or your manager so that they are aware and can give you advice.
- Do not give out your personal contact details to children or parents/carers; professional communication should always be through a work provided email, setting-approved digital platform or phone number.
- If you are concerned about something you see on social media, such as comments posted by a parent, make sure you report it to your DSL. If you are concerned about content posted by a colleague, follow your setting's allegations policy.
- Staff must be clear on the internal and external reporting mechanism regarding online safety concerns.
- Staff must always involve the DSL who will be able to make decisions about how and when to escalate a concern.
- DSLs and staff should know how to contact:

Local Multi-Agency Safeguarding Hub if they have a safeguarding concern about a child.

The Internet Watch Foundation (IWF) if setting need to report illegal images. (Child sexual abuse material)

The Child Exploitation and Online Protection centre (CEOP) if they are worried about online abuse or the way that someone has been communicating online.

The UK Safer Internet Centre Helpline for Professionals or the NSPCC for further information.

Know how to access the settings whistleblowing policy.

This Policy was adopted on	15th February 2019
Date of review and reviewer	17th May 2019 Angela Hynes
Date of next review	February 2020