Online Safety Policy

Our Centre is aware of the growth of the internet and the advantages this can bring. However, it is also aware of the dangers it can pose, and we strive to support children, staff, and families to use the internet safely.

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

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

The breadth of issues included within online safety is considerable, but can be categorised into three areas of risk:

1. **Content:** being exposed to illegal, inappropriate, or harmful material; for example, pornography, fake news racist or radical and extremist views.
2. **Contact:** being subjected to harmful online interaction with other users; for example, commercial advertising as well as adults posing as children or young adults, and
3. **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images, or online bullying.

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 Electronic Learning Journal 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.

We refer to Safeguarding children and protecting professionals in early year's settings: online safety considerations to support this policy.

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

Online Safety Policy

The types and numbers of devices are monitored by the EYFS Coordinator. 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 unless the device is for working from home purposes. The tablet devices are stored in area cupboards which are secured 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 practitioners and 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.
- Staff access Early Year's Online Safety training via the National Day Nurseries Association (NDNA) E-learning or the Leeds for Learning website. This training is accessed by any new members of staff during their induction process and then annually.
- Only use Bright Beginnings devices to record and /or photograph the children in the setting.
- Do not use personal electronic devices with imaging and sharing capabilities, including, mobile phones, smart watches and cameras.
- 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.
- 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.

- Signposting parents to appropriate sources of support regarding online safety at home. We will share monthly Online Safety Newsletters with staff and parents. The centre subscribed to these in December 2024 and are provided by Knowsley Council
- Parents are offered support to help them talk about online safety with their children using appropriate resources
- Parents are signposted to appropriate sources of support regarding online safety at home and are fully supported to understand how to report an online safety concern
- Staff have access to information and guidance for supporting online safety, both personally and professionally

Managing online relationships

- Practitioners should not add parents of children at your setting as friends online; this can blur professional relationships and put the staff member 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.
- Ensuring all electronic communications between staff and parents is professional and takes place via the official Bright Beginnings communication channels, e.g. Famly and the setting's email addresses and telephone numbers. This is to protect staff, children and parents.
- 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.

Online Safety Policy

Cyber Security

Good cyber security means protecting the personal or sensitive information we hold on children and their families in line with the Data Protection Act. We are aware that cyber criminals will target any type of business including childcare and ensure all staff are aware of the value of the information we hold in terms of criminal activity, e.g. scam emails. All staff are reminded to follow all the procedures above including backing up sensitive data, using strong passwords and protecting devices to ensure we are cyber secure. Staff must access the University of Leeds annual security training to access their university of Leeds email address.

To prevent any attempts of a data breach (which is when information held by a business is stolen or accessed without authorisation) that could cause temporary shutdown of our setting and reputational damage with the families we engage with, we inform staff not to open any suspicious messages such as official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'.

Staff are asked to report these to the manager as soon as possible and these will be reported through the National Cyber Security Centre (NCSC) Suspicious email reporting service at report@phishing.gov.uk

Reviewed by	Angela Hynes
Date	January 2025