E-safety & Mobile Phone Policy

Bright Eyes Childcare accepts that in the 21st Century the internet and social media are inherent to people's lives and important for sharing information as well as a learning tool. However, we are also aware that this global network comes with its own risks and dangers. We therefore set out the following guidelines to protect our children, staff and parents.

The internet is an accessible tool to children in early years settings to extend and develop their knowledge via apps and educational videos. All early year's settings have a duty to ensure that children are protected from potential harm both within and beyond the learning environment. Every effort will be made to safeguard against all risks; however, it is likely that we will never be able to eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children and staff continue to be protected.

Aims of this policy

- To offer valuable guidance and resources to early years settings and practitioners to ensure that they can provide a safe and secure online environment for all children in their care.
- To raise awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many educational and social benefits.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the early years setting.

This policy applies to all staff, children, parents/carers, visitors and contractors accessing the internet or using technological devices on the premises. This includes the use of personal devices such as mobile phones or iPads/tablets which are brought into the setting. This policy is also applicable where staff or individuals have been provided with setting issued devices for use off-site, such as a work laptop or mobile phone.

At Bright Eyes we provide a diverse, balanced and relevant approach to the use of technology. Children are encouraged to maximise the benefits and opportunities that technology has to offer. Children learn in an environment where security measures are balanced appropriately with the need to learn effectively. Our settings understand the importance of our E-Safety Policy.

Our E-Safety Champion is April Turner - The role of the E-Safety Champion in our childcare setting includes:

- Ensuring that the E-Safety Policy and associated documents are implemented, reviewed and kept current.
- Ensuring that all staff are aware of reporting procedures and requirements should an E-Safety incident occur.

Broadband and Age-Appropriate Filtering

Broadband provision is essential to the running of our setting. Many settings now use internet enabled devices, including iPad educational apps and games, to enhance the learning experience of children or as online tools for staff to track and share achievement. For this reason, great care must be taken to ensure that there is a safe and secure internet access, appropriate for both adults and children. Filtering levels are managed and monitored using online software 1.1.1.1 Families powered by Cloudflare.

Email

The setting only provides senior staff members with access to a professional email account to use for all work related business, including communication with parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families. All emails should be professional in tone and checked carefully before sending.

Email is covered by the Data Protection Act (2018) and the Freedom of information Act (2000) so safe practise should be followed in respect of record keeping and security. All staff are aware that all email communications may be monitored at any time. All users must report immediately any email that makes them feel uncomfortable, is offensive, threating or bullying in nature.

Use of Social Networking Sites (advertising or parental contact)

Social networking sites such as Facebook or Instagram can be a useful advertising tool for early years settings and can often be an effective way of engaging with young or hard to reach parents. Due to the public nature of social networking and the inability to keep content truly private, great care must be taken in the management and use of such sites. All children and staff are given the opportunity to decline or accept to be include on our social media platforms at enrolment.

- Identifiable images of children should not be used on social networking sites, without parental permission.
- To maintain professional distance and to avoid unwanted contact, staff should not link their personal social networking accounts to the setting's page.
- Ensure that privacy settings are set to maximum and checked regularly.

All employees are encouraged to decline friendships on social media from current parents on their personal accounts.

Our dedicated social media personal are April Turner and Emily Rowe.

Mobile/Smart Phones/Smart watches

Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of nursery. They often provide a collaborative, well-known device with possible internet access and thus open risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in the setting is allowed.

All smart watches must be switched to "Do not Disturb"

Personal Mobile Devices

Employees/Visitors/Parents are to sign in and out personal mobile phones and devices for their own use. Personal mobile phones are kept in an individual labelled slot in the manager's office and are only to be used in the office or staff room during designated breaks. Employees bringing personal devices into the setting must ensure there is no inappropriate or illegal content on the device.

Bright Eyes is not responsible for the loss, damage, or theft of any personal mobile device.

Bright Eyes Provided Mobile Devices

We provide mobile technologies such as phones, laptops, iPads. These devices should be used in the nursery and during outings. These devices are to be signed in and out of the managers office at the beginning and end of each day. Managers and the senior team are to check each devices history and ensure all photos from the week have been deleted.

Managers are provided with a laptop and may only be used to conduct nursery business outside of the nursery, this laptop should be password protected and stored in a secure place overnight.

All children will be supervised whilst always using these devices. Staff and children are not authorised to download any apps or documents.

Photographs and Video's

Digital photographs and videos are an important part of the learning experience in early years settings and, as such, staff have a responsibility to ensure that they not only educate children about the safe and appropriate use of digital imagery, but also model good practice themselves. As photographs and video's of children and staff are regarded as personal data in terms of the Data Protection Act (2018) we must have written permission for their use from the individual or their parent/carer which is given during enrolment. At Bright Eyes we are aware of the issues surrounding the use of digital media online. Parental/carer permission is regularly kept updated on Famly. Parents/carers and staff are aware that full names and personal details will not be used in any digital media, particularly in association with photographs. The use of videos and cameras is not permitted in Bright Eyes, unless by an authorised member of staff with Bright Eyes equipment and for nursery purposes. When taking photographs/video, staffs ensures that subjects are appropriately dressed and are not participating in activities that could be misinterpreted.

Storage of Images

Images/films of children are stored on the nurseries devices which are password protected. Rights of access to this material are restricted to staff within the confines of the nursery setting. All images are deleted at the end of the week.

Webcams and CCTV

Bright Eyes uses CCTV for security and safety on the outside of the building and car park. The only persons with access to these are the manager April Turner and the landlady Gaynor. Webcams are used by staff for meetings with outside agencies, parents and for relevant training sessions.

Applications (Apps) for recording pupil progress

Bright Eyes Childcare uses the Famly app which allows staff to track and share a child's learning journey online with parents and carers, usually in the form of photographs and text. Famly has considerable benefits, including improved levels of engagement with parents and a reduction in paperwork, but careful consideration must be given to safeguarding and data security principles before use.

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, ensuring that any devices used are appropriately encrypted if taken off site. This is to prevent a data security breach in the event of loss or theft.

Data Storage and Security

In line with the requirements of the Data Protection Act (2000), sensitive or personal data is recorded, processed, transferred, and made available for access in the setting. This data must be accurate; secure; fairly and lawfully process; processed for limited purposes and in accordance with the data subjects rights; adequate, relevant and not excessive; kept no longer than necessary; and only transferred to others with adequate protection.

At Bright Eyes we specify how we keep data secure and inform staff as to what they can/cannot do with regard to data through this E-Saftey policy. ICT enables efficient and effective access to and storage of data for the management team and their staff members.

Bright Eyes uses Famly for all children's data purposes. Only trained and designated members of staff have authority and access rights to input or alter data. Bright Eyes only allows senior staff permission to ensure data is well maintained, secure and that appropriate access is properly managed with appropriate training provided.

All laptops and computers are password protected. All work email accounts are password protected. A secure email facility is available for staffs that need to send confidential information. Passwords should contain at least eight characters and contain upper and lower case letters as well as numbers. Passwords should be easy to remember, but hard to guess. Staff should not share their passwords with anyone; write their passwords down or save passwords in web browsers if offered to do so. Staff should not use their username as a password. Staff should not email their password or share it in an instant message. Staff should change their password if they think someone may have found out what it is.

Staff should be aware of who they are allowed to share information with. Clarification can be obtained from the nursery manager. Sensitive information should only be sent via the secure email system. Don't assume that third-party organisations know how your information should be protected.

The use of unencrypted memory storage devices to store information of a personal sensitive or confidential nature is not permitted.

Staff should only download files or programs from trusted sources, if in doubt they should seek advice from the nursery manager.

Staff should lock sensitive information away when left unattended. Unauthorised people should not be allowed into staff areas. Computer screens should be positioned so that they cannot be read by others who shouldn't have access to that information. Confidential documents should not be left out.

Staff should only take information offsite when authorised and only when necessary. On occasions when this is necessary, staff should ensure that the information is protected offsite in the ways referred to above. Staff should be aware of their location and take appropriate action to reduce the risk of theft. Staff should ensure that they sign out completely from any services they have used, for example email accounts.

Serious Incidents

If a serious incident occurs such as inappropriate content is accessed, the E-Safety incident log is made immediately, the area manager is informed and the use of device is suspended until Bright Eyes has had it checked by a trusted IT technician. Details of ALL E-Safety incidents are recorded by staff and monitored monthly by the nursery Manager.

Below is an example of the incident log, which Bright Eyes keeps stored on a password protected device.

E-Safety Incident Log

Date of incident	Name of individual(s) involved	Device details	Details of incident	Action and reasons	Checked by

Signed Nursery Manager:

20th September 2025