On-line Safety

Policy statement

Information Communication Technology has evolved over the years and new and more advanced technologies appear every day. Children and young people are the first to embrace this new culture, however, as adults keeping up with these changes can be a daunting experience. It is for this reason it is important, both as parents and carers, we understand these new technologies and the risks involved in using them. The on-line world is here to stay and with it risks which need to be managed by reducing availability, restricting access, and increasing resilience to keep our children safe online.

The aim of this policy is to:

- Set out the key principles expected of all adults at Mr Bee's with respect to the use of technologies.
- Safeguard and protect the children and staff.
- Assist adults working with children to work safely and responsibly with technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of technologies for educational, personal, or recreational use for the whole Mr Bee's community.
- Have clear structures to deal with online abuse such as online bullying.
- Ensure that all employees are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary, or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with children.

The main areas of risk for use of online technologies can be summarised as follows:

- **Content**: anything posted online – it might be words, or it could be an image or video. Children and young people may see illegal, inappropriate, or harmful content when online. This includes things like pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

- **Contact:** is about the risk of harm young people may face when interacting with other users online. This includes things like peer-to-peer pressure or seeing inappropriate commercial advertising.

Sometimes adults pose as children or young adults with the intention of grooming or exploiting a child or young person for sexual, criminal, financial or other purposes.

- **Conduct:** means the way people behave online. Some online behaviour can increase the likelihood, or even cause, harm – for example, online bullying. Conduct also includes things like sharing or receiving nudes and semi-nude images and view or sending pornography.

- **Commerce**: is about the risk from things like online gambling, inappropriate advertising, phishing, or financial scams. Children and young people may be exposed to these risks directly. Schools should also consider how the risk from commerce applied to staff.

This policy applies to all members of the Mr Bee's community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of childcare technologies, both in and out of Mr Bee's Family Centre.

Procedures for On-line Safety

1. Communication:

This policy will be communicated to employees, volunteers, students, children, and families in the following ways:

- Policy is posted on the Mr Bee's website/staff room and parent boards.
- Policy is part of recruitment pack for new staff.
- All staff must read and sign the 'Code of Conduct' before using any Mr Bee's technology resources.
- Regular updates and training on online safety for all staff, including any revisions to the policy.
- On-line Code of Conduct to form part of long-term planning and to be discussed with staff and pupils at the start of each year.
- On-line Code of Conduct to be issued as part of the registration documents in the Mr Bee's Welcome Pack.

2. Handling Concerns:

- Mr Bee's will take all reasonable precautions to ensure online safety is in line with current guidance from the Department for Education (DfE).

- Staff members and families are given information about infringements in use and possible sanctions which is outlined in the On-line and Employee Code of Conduct.
- Designated Lead Practitioner (SLP) acts as first point of contact for any safeguarding incident whether involving technologies or not.
- Any concern about staff misuse is always referred directly to the Senior Early Years Professional unless the concern is about the Senior Early Years Professional in which case the concern is referred to the Board of Trustees.

3. Review and Monitoring:

- The On-line Safety policy (formerly referred to as the E-Safety policy) is referenced within other the Safeguarding and Child Protection policy.
- The online safety policy will be reviewed annually **or** when any significant changes occur regarding the technologies in use within Mr Bee's.
- There is widespread ownership of the policy, and it is agreed by the Senior Early Years Professional at Development Meetings alongside Centre Leads and approved by the Board of Trustees. All amendments to the Mr Bee's online safety policy will be disseminated to all members of staff and families as outlined in the Mr Bee's Policy Review policy).

4. Education and Curriculum:

Children:

- Children do not normally have access to the internet and never have unsupervised access.
- Parents are asked to read and sign our On-Line Code of Conduct for Parents/Carers which are included in our registration form and outlines how the internet may be used and safety measures put in place, as well as an agreement for parents/carers to support safe use of the internet at home.
- A copy of this policy is available to parents on our website and is sent to parents when reviewed.
- All Mr Bee's computers are locked with a password which is not known to the children.
- Nursery children are not permitted to access online safety education programmes without a member of staff always sitting and supporting them and only reputable sites with a focus on early learning are used (e.g. CBeebies).
- Video sharing sites such as YouTube are not accessed due to the risk of inappropriate content.
- An Out of School age child must be able to understand the Mr Bee's Online Code of Conduct and a risk assessment completed to ascertain whether access is with or without an adult in attendance.

- When an Out of School child requests access to the computer, a staff member will ensure an on-line code of conduct agreement has been read with the child before logging onto the computer and will be taught the following stay safe principles in an age-appropriate way prior to using the internet;
    - only go online with a grown up
    - be kind online and keep information about me safely
    - only press buttons on the internet to things I understand.
    - tell a grown up if something makes me unhappy on the internet.

- All staff will also seek to build children's resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
- All staff members are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright and should discuss with their line manager if they are unclear of these responsibilities.
- All staff members and pupils understand issues around plagiarism; how to check copyright and know that they must respect and acknowledge copyright/intellectual property rights and should discuss with their line manager if they are unclear of these responsibilities (see web address link at back of policy).
- All computers for use by children are sited in an area clearly visible to staff.

Employee and Trustee:

Mr Bee's:

- Makes regular up to date training available to staff on on-line safety issues through Norfolk County Councils training directory and attendance is identified at supervision and appraisal.
- Ensures information from training is cascaded to all staff members through staff, development, and trustee meetings.
- Provides, as part of the induction process, all staff to read the Online Safety Policy and Mr Bee's Code of Conduct and On-line Code of Conduct and agrees to follow by signing.
- The Centre Lead ensures staff members have access to age-appropriate resources to enable them to assist children to use the internet safely.

Parent/Carer:

Mr Bee's:

- posts a copy of the On-line safety policy on the Mr Bee's website for parent/carers.
- Parent/carers are informed when On-line safety policy is due for review and an e-copy sent once reviewed to keep them up to date with changes.
- Signposts parents to information and guidance on online safety such as 'share aware'.

5. Incident Management

At Mr Bee's:

- there is strict monitoring and application of the online safety policy, including the On-line Code of Conduct for families and Code of Conduct for employees and a differentiated and appropriate range of sanctions.
- Staff reports any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.
- Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk**.**
- If staff become aware that a child is the victim of cyber-bullying, they discuss this with their parents and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk.
- support is actively sought from other agencies as needed (i.e. the local authority, Police, NEN) with online safety issues.
- monitoring and reporting of online safety incidents take place and contribute to developments in policy and practice in online safety by requesting a change in policy and procedure. parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- the Police will be contacted if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law
- we will immediately refer any suspected illegal material to the appropriate authorities – i.e. Police, Internet Watch Foundation and inform the LA

6. Use of Electronic Communication:

Mr Bee's:

- Provides each centre with an email account for their professional use which is not to be used for personal email.

- Use Famly, a cloud-based management software programme to communicate securely with employees and parents and is accessed by an individual identification and passwords only known to the user.
- Sensitive or confidential information will not be sent using Famly.
- Arranges for the Senior Early Years Professional and Centre Lead to set the permission for staff members which varies depending on their roles and can change these and/or delete a user if Famly is being used inappropriately or for personal use.
- Will ensure Centre Leads maintain Famly accounts and keep them up to date for their centre, especially when a staff member or parent leaves Mr Bee's.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

Email:

- Children are not permitted to use email in the Centre,
- Parents are not normally permitted to use Centre equipment to access personal emails.
- Staff will use individual or centre emails for professional purposes only.
- Access to external personal email accounts is not permitted using Mr Bee's computers and / or electronic devices.
- Never use email to transfer staff or pupil personal data unless it is protected with secure encryption. 'Protect-level' data should never be transferred by email. If there is no secure file transfer solution available for the situation, then the data / file must be protected with security encryption.

7. Mr Bee's Website:

- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs of pupils published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

8. Mr Bee's Devices:

- Centre Leads will ensure all Mr Bee's electronic devices are labelled with centre information to show they are work related IT equipment.
- All Mr Bee's electronic devices are recorded on the Centre IT Audit.
- If a second-hand computer is purchased or donated to the Centre, the Centre Lead will seek authorisation to use by Senior Early Years Professional or Trustee and ensure that no inappropriate material is stored on it before children use it.
- All devices for use by children are in an area clearly visible to staff.
- The Centre Leads ensures that all computers have up-to-date virus protection installed on any device used in the centre.
- Tablets are only used for the purposes of observation, assessment, and planning and to take photographs for individual children's learning journeys.
- Tablets remain on the premises and are always stored securely when not in use.
- Staff follow the additional guidance provided with the system.

9. Guidance for 'Bring Your Own Device':

Employees:

- Personal devices cause disruption and distraction which means children are not given the full attention of staff members. They also provide an easy way of taking images which can be sent directly to the internet and used in email. It is for this reason staff members leave their own devices switched off and locked in their person locker in the staff room or the centre office.
- Personal mobile phones and internet enabled devices are not used by staff during working hours. These are only permitted during designated breaks and areas where children are not in attendance. The Centre Lead completes a risk assessment for where they can be used safely.
- In an emergency, staff members ensure family members know how to contact them on the main number of the centre in which they are working or with permission of the Centre Lead/Supervisor, use in the privacy of the office.
- Personal devices are not permitted on outings and school runs and will be left at the individual centres as outlined above unless approval has been given by the line manager. Approval will only be given in emergency situations for a limited period. Reasons are to be confidentially logged on the staff members file together with the control measures put in place and authorised by the Senior Early Years.
- Members of staff do not use personal equipment to take photographs of children.
- Must not view inappropriate images at any time during working hours (see Code of Conduct).

- Personal devices should not be used during training sessions and must be kept out of reach and/or sight unless permission has been sought and approved by a Senior Manager and /or the trainer.

Children:

- will leave personal devices in their bags (working or otherwise) unless a risk assessment has been completed and control measures identified and agreed by Centre Lead and parent.
- If a child takes device out of bag without a risk assessment having been put in place, the device will be removed and stored in the office until the parent collects them at the end of the session.

Parents:

- will be asked not to use their mobile phones in the childcare rooms and signs displayed. If a parent attempts to use their mobile phone, any staff member present must politely ask them to leave the room and draw their attention to our safety notice.
- Where parents request permission to photograph or record their own children at special events, general permission is first gained from all parents for their children to be included. Parents are told they do not have a right to photograph or upload photos of anyone else's children.

Visitors:

- will be politely asked to leave their electronic devices in the office. However, it is recognised that some visitors may be on call for child protection related matters and need to be available quickly in an emergency. In this case, a mobile phone permission slip must be completed and stapled into the centre's diary.
- The visitor is told they may keep their phone on them, but they must use their mobile phone where no children are present.
- The above rule also applies to the use of work-issued mobiles, and when visiting or supporting staff in other Centres.

Centre Leads:

- complete a device risk assessment which will identify areas which may permit parents/visitors to take images without the knowledge of staff members (i.e. through the window of parent rooms, perimeter fences, etc.) and outline the control measures put in place.
- Ensure home visit risk assessment includes control measures put in place if a personal device is required during home visits for a staff member's safety (see Lone Worker Policy) or for translation purposes.

Senior Managers:

- are permitted to use personal mobile phones for work purposes but these are not permitted in the childcare rooms with children present.

10. Digital Images and Video:

- Our staff and volunteers must not bring their personal cameras or video recording equipment into the Centre.
- Consent by parents for images and how information is to be used is outlined on our registration form and Keeping Children Safe in the Early Years Leaflet. Some parents may have made requests for photographs not to be taken - each room has a list of children who may need to be excluded from taking photographs and practitioners are responsible for ensuring they know the whereabouts of this list. In the case of a looked after child, permission must be obtained from the child's social worker and not their carer.
- Photographs and recordings of children are only taken for valid reasons, for example, to record their learning and development, or for displays within the Centre. Written permission will be received by parents for any other reason (please refer to save use of images section in our Keeping Children Safe in the Early Years leaflet and image consent form on registration form).
- If photographs are used for publicity, parental consent is gained and safeguarding risks minimised, e.g. children may be identified if photographed in a sweatshirt with the name of their setting on it.
- Images on cameras are confidential and must be treated as such. Images are not permitted to leave the premises without the consent of the Centre Lead or Lead Practitioner and then only under the guidelines set out in the Mr Bee's Children's Records and Key Person Role and Settling in Policies.
- Images taken during outings are only taken using a Mr. Bee's device. Any images already on the camera must be uploaded onto the centre computer and deleted from the camera before leaving the Centre.
- Images may only be uploaded onto a computer by the Room Lead or a more senior member of staff who will check images to ensure they are appropriate for use.
- Images will be stored on the individual centre computers and deleted in line with our Children's Records policy and data protection legislation.
- When images are required staff members will be sensitive to children who may be uncomfortable with being photographed or filmed and ensure photographs are not taking during intimate care.

There are strictly no devices permitted in areas where children receive intimate care.

11. Social Media:

All employees, volunteers, and students:

- involved with Mr Bee's are instructed to always keep professional and private communication separate and as such ensure the organisation is not negatively affected by their actions and do not declare their place of work on social media (see Code of Conduct).
- Must carefully manage their personal security settings to ensure that their information is only available to people they choose to share information with.
- are aware that comments or photographs online may be accessible to anyone and should use their judgement before posting.
- are aware that images, such as those on Snapshot may still be accessed by others and a permanent record of them made, for example, by taking a screen shot of the image with a mobile phone.
- not share information they would not want children, parents, or colleagues to view.
- set privacy settings to personal social networking and restrict those who can access.
- Staff should not accept service users, children, and parents as friends due to it being a breach of expected professional conduct.
- report any concerns or breaches to the Safeguarding Lead Practitioner (SLP) in their Centre.
- not engage personal communication, including on social networking sites, with the children and parents with whom they act in a professional capacity. If a practitioner and family are friendly prior to the child coming into the Centre, this information is shared with the manager prior to a child attending and a risk assessment and agreement in relation to boundaries is agreed.
- Are instructed not to run social network spaces for child use on a personal basis or to open their own spaces to children but to use the Mr Bee's preferred system for such communication.
- will ensure they follow the Code of Conduct when using approved social networking sites.
- would be easily accessible at the centre is sent (planning, activities, term times and dates, etc.).
- observe confidentiality and refrain from discussing any issues relating to work including any of Mr Bee's employees, volunteers, or families on any social media/networking sites other than Mr. Bee's Family Centre's official sites (see confidentiality policy and confidentiality agreement).
- ensure they are not exposed to any inappropriate images or web links (see Code of Conduct).
- are aware that it is an offence to distribute indecent images and that it is an offence to groom children online. In the event of a concern that a colleague is behaving inappropriately, staff advise the Centre SLP in their Centre who will follow the Allegations and concerns about adults who work with children in the setting which forms part of our Safeguarding children and child protection policy.

Centre Leads and the Senior Early Years Professional will:

- manage the individual Facebook childcare pages for the organisation.
- ensure first names only are used when uploading images onto a Mr. Bee's Facebook page with the appropriate consent for use of images.
- ensure any Facebook related requests which may allow the identification of any person who attends and/or works at Mr. Bee's is not permitted (i.e. tagging).

Children (where appropriate):

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation, or abuse through our online safety curriculum work.
- Students are required to sign and follow our [age appropriate] On-line Code of Conduct.

Parents/Carers:

- Parents/carers are reminded about social networking risks and protocols through our parental Online Code of Conduct and additional communications materials when required.

12. Data Security:

- Refer to Information Sharing and Children's Record policy for management information system access and data transfer.
- All personal information is held securely and in line with the Data Protection Act 2018 including GDPR and guidance from the Information Commissioner's Office (ICO).

13. Non-Compliance:

- Anyone who does not comply with the above policy and procedure will be subject to disciplinary action and / or reporting to relevant agency.
- All employees have a duty of care to keep children safe from harm and therefore must report any non-compliance by following the Whistle Blowing policy.

Legal framework

- 1989 Children Act (Section 17 and 47)
- 2004 Children Act (Section 10 and 11)
- Protection of Children Act (1999)
- Data Protection Act (2018) including General Data Protection Regulations (GDPR)
- Safeguarding Vulnerable Groups Act (2006)

Further Guidance

- NSPCC and CEOP *Keeping Children Safe Online* training: www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/
- Working Together to Safeguard Children (2023)
- Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents, and carers (July 2018)
- Norfolk County Council Safeguarding Children in the early years and childcare (June 2012)
- Mr. Bee's Information for Parents and Carers: Keeping Children safe in Early Years Education
- Mr Bee's Visitors Information Leaflet
- https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware
- http://www.nen.gov.uk/online-safety

Forms:

- Mobile phone permission slip
- Image Consent Form (Famly Permissions)
- Keeping Children Safe in the Early Years Leaflet (Mr Bee's website)
- Visitor Signing in Sheet
- On-Line Code of Conduct Parent/Carer (Famly Permissions)
- Employee, Volunteer, Trustee and Visitor ICT Code of Conduct

Linked policies:

- Confidentiality, recording, information sharing and Client Access to records
- Lone Worker Policy
- Children's Records
- Provider Records
- Key Person Role and Settling in
- Safeguarding Children and Child Protection
- Whistle Blowing
- Childcare Privacy Notice
- Employee Privacy Notice

Re: On-line Safety

This policy was reviewed at a meeting of	Mr. Bee's Family Centre
Held on	26th March 2024
Date to be reviewed	March 2027

Signed on behalf of the Board of Trustees:	
Name of role of signatory:	Jeanette Nowrung, Chairperson
Signed by Senior Early Years Professional:	
Individual Centre Lead's Signature:	
North Lynn:	
Springwood:	
St Augustine's:	