Safeguarding children

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 on line.

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 on line technologies can be summarised as follows:

Content:
- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

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 (Childcare) or Operational Manager (Operational), unless the concern is about the Senior Early Years Professional or Operational Manager 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 with regard to the technologies in use within Mr Bee's.

- There is widespread ownership of the policy and it has been agreed by the Senior Early Years Professional, Operational Manager 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:

Pupil:
- 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 programme without a member of staff sitting and supporting them at all times.

- An Out of School age child must be able to understand the Mr Bee's On Line 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.

- 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 also 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).

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.

Parent/Carer:

Mr Bee's:

- posts a copy of the Online safety policy on the Mr Bee's website for parent/carers.
- Parent/carers are informed when Online 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'.

4. 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.

- support is actively sought from other agencies as needed (i.e. the local authority, NSPCC, Police, NEN) with online safety issues.

- monitoring and reporting of online safety incidents takes 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

5. 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 Parentmail to communicate securely with employees and parents and is accessed by an individual identification and passwords only known to the user.
- Arranges for the Senior Early Years Professional and Centre Lead to set the permission for staff members which varies depending on their roles and is able to change these and/or delete a user if parentmail mail is being used inappropriately or for personal use.
- Will ensure Centre Leads maintain parentmail 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.

Staff email:
- Staff will use individual or centre emails for professional purposes only.

- Access in school 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.

6. 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;

7. 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.

8. 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 locked in their person locker in the staff room or the centre office.
- Only use personal devices during designated breaks and areas where children are not in attendance. In an emergency, family members can contact the main number of the centre in which they are working.
- 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 of time. 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 Professional (childcare) or Operational Manager (operational).
- 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.

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.

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 leave the room when answering a call.

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.

9. Digital Images and Video:

- Consent for images is provided by parents and 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.
- 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 Leader 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.

10. 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 are not permitted to declare their place of work on social media (see Code of Conduct).
- Are instructed not to run social network spaces for child use on a personal basis or to open up 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.
- When using text, email or Parentmail to communicate with a parent, personal or confidential information must not be sent. If a parent requests updates on their child's daily routine and events to be sent by text or email, staff members ensure only the information requested by the parent at the front of the communication book and/or information which would be easily accessible at the centre is sent (planning, activities, term times and dates, etc).
- Information regarding Mr. Bee's, any of its employees, volunteers or families is not permitted 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).

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.

11. Data Security:

Refer to Information Sharing and Children's Record policy for management information system access and data transfer.

We are currently seeking guidance from our IT Support company to ensure we are fully compliant with the General Data Protection Regulations which is mandatory from 25th May 2018.

12. 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 (1998)
- Safeguarding Vulnerable Groups Act (2006)

Further Guidance

- Working Together to Safeguard Children (March 2015)
- Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers (HMG March 2015)
- 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
- http://carolsimpson.com/copyright/Copyright%20and%20plagiarism%20guidelines%20for%20students.pdf
- https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware
- http://www.nen.gov.uk/online-safety
- NEN – The Education Network: School e-Security Checklist (Nov 2014)

Forms:

Mobile phone permission slip
Image Consent Form
Visitor Signing in Sheet
On-Line Code of Conduct

Linked policies:

Code of Conduct
Lone Worker Policy
Children's Records

Key Person Role and Settling in
Safeguarding Children and Child Protection
Whistle Blowing
Information Sharing

Re: On-line Safety

This policy was adopted at a meeting of | Mr. Bee's Family Centre | name of setting

Held on | 9th June 2017 | (date)

Date to be reviewed | June 2019 | (date)

Signed on behalf of the management committee

Name of signatory | Jeanette Nowrung

Role of signatory (e.g. chair/owner) | Trustee

Centre Manager's Signature: