Safeguarding children, young people and vulnerable adults Procedures

6.9 E-Safety

Policy statement

It is important that children and young people receive consistent messages about the safe use of technology and are able to recognise and manage the risks posed in both the real and the virtual world.

Terms such as ‘e-safety’, ‘online’, ‘communication technologies’ and ‘digital technologies’ refer to fixed and mobile technologies that adults and children may encounter, now and in the future, which allow them access to content and communications that could raise issues or pose risks. The issues are:

Content – being exposed to illegal, inappropriate or harmful material

Contact – being subjected to harmful online interaction with other users

Conduct – personal online behaviour that increases the likelihood of, or causes, harm

An E-safety audit is included in these procedures to assist with compliance to the revised EYFS 2025.

Procedures

I.C.T Equipment

- The setting manager ensures that all computers have up-to-date virus protection installed.
- Tablets are only used for the purposes of observation, assessment and planning and to take photographs for individual children’s learning journeys.
- Tablets may be used to take photographs when on outings.
- Tablets are password protected.

- Tablets are used for to access Blossom Educational (online observational system). Blossom Educational protect all data and privacy. All of data is stored on secure servers and back-ups are made in real-time. TSL technology is used to ensure there is a secure connection so only the setting can view the Jack and Jill Nursery information. All of the passwords are encrypted to ensure protection over your data. The core of Blossom Educational's data resides with Amazon Web Services (AWS), a cloud based data center. They are compliant with ISO standards 9001:2008 and 27001:2013 and have passed the PCIDSS v3 certification. All devices must be authorised by manager/deputy manager. Staff are given limited access levels.
- Tablets remain on the premises and are always stored securely when not in use.
- The Manager and deputy manager will occasionally use the Blossom Educational website at home using their work computers.
- Parents can access their children's details and learning observation photographs by using the Blossom educational app, available on iOS and Android.

Internet access

- Children never have unsupervised access to the internet.
- Only reputable sites with a focus on early learning are used (e.g. CBeebies).
- Children are taught the following stay safe principles in an age appropriate way:
  - 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
- Staff support children's resilience in relation to issues they may face online, and address issues such as staying safe, appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age-appropriate ways.
- All computers for use by children are sited in an area clearly visible to staff.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.

The setting manager ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.

Strategies to minimise risk include:

- Check apps, websites and search results before using them with children.
- Children in Early Years should always be supervised when accessing the internet.
- Ensure safety modes and filters are applied - default settings tend not to ensure a high level of privacy or security. But remember you still need to supervise children closely.
- Role model safe behaviour and privacy awareness. Talk to children about safe use, for example ask permission before taking a child's picture even if parental consent has been given.
- Make use of home visits to inform your understanding of how technology is used within the home and the context of the child with regards to technology.
- Check privacy settings to make sure personal data is not being shared inadvertently or inappropriately. (source: https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-guidance-for-practitioners

Personal Mobile Phones, internet enabled devices and those with sharing and imaging capabilities – staff and visitors

- Personal mobile phones, internet enabled devices and all electronic devices with sharing and imaging capabilities are not used by staff during working hours.
- During the hours of 12.30pm and 1pm, mobile phones can briefly be looked at, in the manager's office with the door closed. If a member of staff, student or visitor, needs to check their phone outside of these hours, permission must be gained by the manager/deputy manager.
- In the event of an emergency, personal mobile phones may be used in the privacy of the office, with permission from the manager.
- Personal mobile phones are switched off or to silent and stored in the locked box in the manager's office.
- All mobile phones should be password protected and insured. The setting accepts no liability for loss, damage or theft.
- Staff ensure that contact details of the setting are known to family and people who may need to contact them in an emergency.
- Members of staff do not use personal equipment to take photographs of children.
- Parents and visitors do not use their mobile phones on the premises. There is an exception if a visitor's company/organisation operates a policy that requires contact with their office periodically throughout the day. Visitors are advised of a private space where they can use their mobile.

- The manager/deputy manager may use their mobile phones whilst in the office for work purposes when appropriate, during the working day.
- All personal mobile phone use is open to scrutiny and the management can withdraw or restrict authorisation at any time.
- All members of staff, students and visitors must be aware that under no circumstances should personal mobile phones, internet enabled devices and any electronic devices with sharing and imaging capabilities be used to record, photograph or video children within the setting or on outings.
- One mobile phone may be taken on outings, for use in the case of an emergency, they must not take photographs of the children, make or receive personal calls as this may distract them from their duties.
- An E-safety audit is included in these procedures to assist with compliance to the revised EYFS 2025.

Cameras and Videos

- The taking of photographs and videos is monitored by the setting manager/deputy manager.
- Photographs or videos of children are only taken on equipment belonging to the setting.
- Photographs and videos of children are only taken for valid reasons.
- The setting requires all parents/carers to sign the consent to taking of photographs form before their child joins the setting. Photographs/recordings of children are only made if relevant permissions are in place.
- Children are given the opportunity to consent to their photograph being taken, even if parent/carer permissions are in place.
- If photographs are needed for any other purpose, for example, practitioners and students course work, external press releases, or if parents wish to take photographs or videos at Easter or Christmas celebrations the setting will request direct written permission from parents/carers.
- Photographs that are taken and stored on the settings cameras/iPads/tablets must be downloaded and printed off or uploaded to the online learning journal as soon as possible, and then deleted off the memory card/device; ideally this should happen once a week.
- All video recordings unless needed to be viewed by outside agencies (with parental permission) will also be deleted off the memory cards/devices.

Cyber Bullying

If staff become aware that a child is the victim of cyber-bullying at home or elsewhere, they discuss this with the parents and refer them to help, such as: NSPCC Tel: 0808 800 5000 www.nspcc.org.uk or ChildLine Tel: 0800 1111 www.childline.org.uk

Use of Social Media

Staff (and student and volunteers) are expected to:

- understand how to manage their security settings to ensure that their information is only available to people they choose to share information with
- ensure the organisation is not negatively affected by their actions and do not name the setting
- are aware that comments or photographs online may be accessible to anyone and should use their judgement before posting
- observe confidentiality and refrain from discussing any issues relating to work
- not share information they would not want children, parents or colleagues to view
- set privacy settings to personal social networking and restrict those who are able to access
- not accept service users/children/parents as friends, as it is a breach of professional conduct
- report any concerns or breaches to the designated safeguarding lead person in their setting
- not engage in personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. There may be occasions when the practitioner and family are friendly prior to the child coming to the setting. In this case information is shared with the manager and a risk assessment and agreement in relation to boundaries are agreed
- must not engage in any activities which may harm the welfare of children or adults in connection with the setting and that their duty to safeguard children is maintained.
- must not disclosing any information regarding children or staff (written or pictorial), and other confidential information regarding the setting.
- should bear in mind that information they share through social networking applications, even though they are on private spaces, are still subject to copyright, data protection and freedom of information legislation, the safeguarding vulnerable groups act 2006 and other legislation.
- must not post comments that can be interpreted as:
    - Personal attacks
    - Defamation
    - Bullying and harassment
    - Spam
    - Offensive comment
    - Illegal activities.

- Any misuse of social networking sites that has a negative impact on the setting may be regarded as a disciplinary offence. Instances where the setting is brought into disrepute may constitute misconduct or

gross misconduct and disciplinary action will be applied (Please refer to the Staff Disciplinary and Grievance Procedures).

If any Members of staff, volunteers or students believe something has been written which gives rise to concern, these concerns should immediately be reported to the manager; if it is inappropriate to make such a disclosure to the manager, concerns should be directed to the deputy manager, Surrey Early Years or Ofsted (see whistle blowing policy).

Use/distribution of inappropriate images

- Staff 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 designated safeguarding lead who follows procedure 06.2 Allegations against staff, volunteers or agency staff.

This policy was updated on the 25th July 2025 by Susannah Townley, Manager.

This policy is due to be reviewed on the 23rd July 2026.