Safeguarding and Welfare Requirement: Child Protection

Online safety (inc. mobile phones and cameras)

Policy statement

Children's online safety and protection from harmful or inappropriate digital content is a fundamental safeguarding responsibility.
We ensure that the use of Information Communication Technology (ICT), mobile phones, cameras, learning platforms and digital devices is safe, controlled, and consistent with legislation and best practice.

We recognise that online risks include:

- exposure to harmful content,
- grooming or online contact from unknown adults,
- cyberbullying,
- image misuse,
- live-streaming,
- inappropriate sharing of personal information,
- radicalisation, extremism, or discriminatory content.

We take proactive steps to:

- prevent exposure to risks,
- teach children age-appropriate online safety,
- safeguard personal data,
- support staff in safe professional conduct, and
- meet all statutory duties under the EYFS and BSCP

Roles and Responsibilities

Designated Safeguarding Lead (DSL):

- Emily Foote (Deputy Manager)
- Lucy Hawkins (Deputy Manager)

The DSL oversees all matters relating to online safety, ICT security, and digital safeguarding.
The DSL ensures:

- risk assessments are completed annually or after any incident,
- staff receive up-to-date training,
- all digital equipment is secure and safe to use,
- safe systems prevent children accessing harmful content,
- any incident or concern is recorded and acted on promptly.

Safeguarding and Welfare Requirement: Child Protection

Information Communication Technology (ICT) equipment

- Only setting-owned ICT devices are used by staff or children.
- All devices are maintained, password protected, and encrypted where appropriate.
- The DSL ensures:
  - all equipment is safe,
  - antivirus/anti-malware software is active,
  - internet filters and safety settings prevent access to inappropriate content,
  - software and systems are regularly checked and updated.
- Staff must not install unauthorised software or apps on setting devices.
- Second-hand or donated equipment must be checked by the DSL to ensure no inappropriate content or unsecured data remains.

Internet Access and Online Learning

- Children do not have unsupervised access to the internet.
- Any online activity is age-appropriate, supervised, and risk assessed.
- Children are taught simple "stay safe online" rules, including:
  - "Only go on the internet with a grown-up."
  - "Only click on things I recognise and understand."
  - "Tell a grown-up if something makes me feel upset or worried."
- **Content restrictions**
  - Children cannot access social networking sites, video-sharing platforms, chatrooms, or live-streaming content.
  - Staff report any online safety concerns immediately to the DSL.
- **Reporting harmful material**
  - Harmful or illegal online content can be reported to the Internet Watch Foundation.
  - Concerns of grooming or inappropriate contact online are reported to CEOP (National Crime Agency).
  - Radicalisation/extremism concerns follow the Prevent Duty procedures.
- **Cyberbullying**

If staff become aware of cyberbullying involving a child:

  - the DSL informs parents sensitively,
  - the concern is recorded,
  - families may be signposted to support such as NSPCC or Childline.

Safeguarding and Welfare Requirement: Child Protection

Email and Digital Communication

- Children do not access email within the setting.
- Staff must not access personal email accounts while supervising children.
- Sensitive information is shared only through **secure, encrypted** communication systems authorised by the Manager.
- Staff must never send child images or data to a personal device or personal email address.

Mobile phones – children

- Children must not bring mobile phones or ICT devices into the setting.
- If a device is found, it is safely stored and returned to the parent at collection.
- Any repeated issue may lead to a safeguarding conversation with the family.

Mobile phones – Staff, Volunteers and Visitors

Staff and Volunteers

- Personal mobile phones must not be used in the setting during working hours.
- Phones must be stored in a secure staff area, not carried on the person.
- In emergencies, staff may use their phone only in a child-free area and with the Manager's permission.
- Staff must not:
  - use phones in classrooms, bathrooms, changing areas, or outdoor play spaces
  - take photos/videos on personal devices
  - use messaging apps during working hours
- Staff ensure that family members use the setting telephone number for contact during the day.

Outings

- A work mobile phone is taken on outings for emergencies only.
- Staff phones may be carried only with Manager approval and must not be used to photograph children or make personal calls.

Parents and Visitors

- Parents and visitors are asked not to use mobile phones inside the setting.
- Where a visitor's organisation requires phone access for lone working, they may use a designated child-free area under supervision.

Safeguarding and Welfare Requirement: Child Protection

Cameras, Videos and Digital Images

Staff Cameras

- Staff must never bring personal cameras or recording equipment into the setting.
- Only setting-owned cameras/devices are used for taking photos of children.

Use of Images

- Photographs are taken only:
  - for recording learning and development,
  - for displays within the setting,
  - for the child's learning journal,
  - for pre-approved publicity with separate consent.

  Parent written consent is required before any images are taken.
- Images are stored securely and deleted when no longer needed.
- Children will not be identifiable by name in publicity images.
- Children must not be photographed wearing clothing that identifies the setting (e.g., logo jumpers) for publicity.

Parents Taking Photos at Events

- Parents may photograph only their own child unless all parents have consented.
- Parents may not post photos or videos of other children online or share them outside their family.

Social Media and Staff Conduct

- Staff must manage privacy settings to protect personal information.
- Staff must not:
  - accept parents, carers, or children as social media friends,
  - share information about work, children, or colleagues,
  - post photos relating to the setting,
  - make negative or harmful comments about the organisation,
  - message families through personal accounts,
  - discuss confidential matters online.
- Any pre-existing relationship between a staff member and a family must be declared to the Manager.
  - A written risk assessment and professional boundaries agreement will be completed.
- Any breach must be reported to the DSL immediately.

Safeguarding and Welfare Requirement: Child Protection

Electronic learning journals

Where an online learning journal platform is used:

- The Manager completes a data protection and online safety risk assessment.
- Staff follow all platform security guidance.
- Images must only be uploaded using setting devices.
- Parent access is password-protected and monitored.
- Staff must not download or store images on personal devices.

Inappropriate Images and Online Abuse

- It is an offence to make, possess, or distribute indecent images of a child.
- Any concern that a staff member or visitor is using, storing, sharing, or accessing inappropriate images is treated as a safeguarding allegation and managed under our Allegations Against Staff Procedure.
- Concerns about grooming, sexual communication or online harm are reported to:
    - Police,
    - CEOP,
    - Bromley MASH (if applicable).

All incidents are recorded and reported in line with statutory requirements.

Training and Monitoring

- Staff receive regular online safety training, including NSPCC/CEOP.
- Online safety is included in induction, supervision, and annual refreshers.
- The DSL reviews this policy annually and after any incident.
- Online safety is discussed with children in age-appropriate ways.
- The Manager monitors the secure use of devices, images, and permissions.

Policy Review

This policy is reviewed:

- annually,
- after any safeguarding incident,
- following changes in legislation, guidance, or BSCP recommendations.