1.10 Mobile phones, electronic devices, media and social networking

Policy

We take steps to ensure that there are effective procedures in place to protect children, young people, vulnerable adults and the setting/ company from the unacceptable use of mobile phones, electronic devices, any content and/or social networking.

Procedures

Personal mobile phones

- Staff must ensure that personal mobile phones belonging to our staff and volunteers are not carried about their person during working hours and are stored in lockers or locked away, although these can be used in the staff room(s) during rest and lunch breaks or outside away from the premises.
- Personal mobile phones are not used on the premises during working hours.
- At the beginning of each individual's shift, personal mobile phones are stored in lockers or locked away in the staff room. Mobile phones cannot be left out, unsupervised or left on charge. We ask that these are turned off or put on silent.
- In the event of an emergency, personal mobile phones may be used in privacy, where there are no children present, with permission from the manager
- Our staff and volunteers ensure that the work telephone number is known to their immediate family and other people who need to contact them in an emergency.
- Where trips are taken outside of the setting a company mobile phone is provided by the manager. Staff may take a personal mobile and use in emergencies. We advise that the electronic devices used are fully charged and switched on for the duration of the trip and contact details shared with working colleagues.
- If our members of staff or volunteers take their own mobile phones on outings, for use in the case of an emergency, they must not make or receive personal calls as this will distract them. (Nor should they use their personal device for anything other than an emergency.)
- Using any personal mobile phones (or other electronic devices) to take pictures or video clips of children is not allowed.
- Our staff and volunteers will not use their personal mobile phones for taking pictures or videos of children on outings.
- Parents and visitors are requested not to use their mobile phones whilst on the premises. There is an exception if a visitor's company or organisation operates a lone working policy that requires contact with their office periodically throughout the day. Visitors will be advised of a quiet space where they can use their mobile phone where there are no children present and accompanied by a member of the management team.

Electronic Devices

The use of electronic devices (*for example: phones, cameras, computers, tablet computers, laptops, music players, game consoles, removable storage devices, memory cards, USB pens, smart watches, video cameras and/ or any similar devices*) could expose children in the setting's care to potential safeguarding risks and could distract people from full supervision and interaction with the children as well as portraying an unprofessional image to parents and visitors. Therefore, the following rules on personal and company electronic devices apply:

Personal Electronic Devices

- The use of personal electronic devices whilst on duty within the childcare environment is strictly forbidden.
- Staff must ensure that personal devices are not carried about their person during working hours and are stored in lockers or locked away, although these can be used in the staff room(s) during rest and lunch breaks or outside of the premises.
- At the beginning of each individual's shift, personal devices are stored in lockers or locked away in the staff room. Electronic Devices cannot be left out, unsupervised or left on charge. We ask that these are turned off or put on silent.
- Using any personal electronic device to take pictures or video clips of children is not allowed.
- If our members of staff or volunteers take their own electronic devices on outings, they must not use them when responsible for a group of children as this will distract them.
- Parents and visitors are requested not to use their personal device whilst on the premises. There is an exception if a visitor's company or organisation operates a lone working policy that requires contact with their office periodically throughout the day. Visitors will be advised of a quiet space where they can use their electronic device where there are no children present and accompanied by a member of the management team.
- Personal electronic devices must not be used to purchase online, goods or products, register to subscriptions, or download apps with the company's details unless authorised by a manager or director.
- Employees are not permitted to spend '*contracted time'* on personal devices for personal matters *(for example: arranging a holiday, shopping, looking at personal interest websites).*

Company Electronic Devices

- Electronic devices and ICT equipment are supplied and owned by the setting.
- Any electrical devices supplied by the setting are not to be taken home. (Unless permission is given by a member of the management team)
- Any electronic device broken will be investigated and if applicable the setting have employees consent to make 'authority to make deductions'.
- Children are supervised when using electronic devices.
- Where trips are taken outside of the setting company electronic devices may be used if authorised by the manager. We advise that the electronic devices used are fully charged.
- Photographs and recordings of children are only taken for valid reasons, *(for example: to record their learning and development, for displays within the setting, or to record class event).*
- Camera and video use is monitored by the setting's director(s) manager(s) and room supervisor(s).
- Company electronic devices must not be used to promote or run other commercial businesses.
- Company electronic devices must not be used to download unauthorised content or distribute games, music or pictures from the internet for personal use. They can bring viruses with them, use up capacity on the servers and potentially breach copyright.
- Company electronic devices must not be used to purchase online goods or products, register to subscriptions, or download apps unless authorised by a director.
- Staff are not permitted to spend '*contracted time'* on personal matters *(for example: arranging a holiday, shopping, looking at personal interest websites)* using company electronic devices.
- Staff and volunteers must access support or training if they are unfamiliar with how to use a piece of equipment or software.
- Staff and volunteers must keep passwords of any device private and confidential.
- Electronic devices must be used in a safe and appropriate manner, and any staff or volunteers found to be mistreating the equipment may result in disciplinary action.

Photographs and Videos

Photographs and videos are an important tool to evidence the development and learning of the children and provide a valuable record of the child's time at the setting; however, they need to be taken safely. The following guidelines should be adhered to:

- Where parents request permission to photograph or record their own children at special events, permission will first be gained from all parents for their children to be included.
- Photographs and recordings of children are only taken of children if parents provide written permission to do so (found on the individual child's registration form on NIAB).
- Pictures can only be taken with devices owned by the setting/ company.
- Pictures and videos should only be stored on the setting's own devices.
- Under no circumstances should staff or volunteers remove pictures or videos from the setting.

Appropriate and Inappropriate Use of Electronic Devices and Platforms

Appropriate Use

The setting encourages it employees to use the variety of devices and platforms which the company own to support and help them to communicate effectively *(for example: phones, intercoms, cctv, the internet, e-mails, calendars, messaging, digital or scanned documents, software, printing*). We expect employees to use such devices and platforms which are associated to their job role and responsibility. The setting support employees using these at work where this can save time and expense.

Staff should ensure that they communicate effectively, be well structured and professional, portraying a good company image. If staff are unsure about a procedure or propose which may breach this guidance then they should seek advice from their line manager and/ or director.

Inappropriate Use

The following are examples of inappropriate use:

- Using the internet to gain access to private social media or emails.
- Printing personal images off at work for home
- Sending or receiving, downloading, or disseminating material that causes insults, offence or harasses others
- Accessing pornographic, racist, or other inappropriate or unlawful material
- Engaging in online chat rooms or gambling
- Inappropriate use of security systems and content (for example: cctv, intercom(s))
- Forwarding electronic chain letters or similar materials
- Sending or receiving messages or phone calls not associated to 'work'
- Transmitting unauthorised confidential information about the children, families, or the organisation
- Downloading or playing computer games (unless authorised)
- Copying copyrighted material owned by the setting
- Downloading software and changing settings. (Unless authorised)
- This is not an exhaustive list.

Social Networking

The setting encourages it employees to use the variety of social networking platforms which the company own to support and help them to communicate effectively *(for example, Facebook, Blog, Website).* However, it requires that employees ensure that their communication is well structured and professional, portraying a good company image. The setting respects employee's right to a private life. However, the setting must also ensure that confidentiality and its reputation are protected. Therefore, when using social networking platforms, the following apply:

- The setting(s) social networking platforms are published in a public domain. This is used to share and network information to and from parents, carers, and nurseries.
- The setting(s) social networking platforms are managed and policed by setting(s) management and directors. It is strictly forbidden for anyone to tamper, edit or try to access the editing package. The setting will contact the police to deal with any cyber-attack or infringement.
- All parents or carers give permission for their child's photograph to be on social networking platforms. Photographs can be sent to parents in advance if they wish it and also can be removed.
- Our staff and volunteers do not create social networking platforms (*for example: page, group, blog, website, app, group message)* or anything associated to the setting or company without a director's permission. You are free to set up personal platforms on the internet, provided that they do not:
    - breach the law,
    - disclose any of the setting's confidential information,
    - breach copyright,
    - defame the company or its suppliers, customers or employees;
    - bring the organisation into disrepute,
    - disclose personal data,
    - disclose information about any individual that could breach the Data Protection Act 1998.
- Our staff and volunteers do not enter into conversation(s) about a child or children. Under no circumstances should children that are currently registered/ or have been cared for by our setting(s) or company be discussed.
- Our staff and volunteers do not search or add new clients of the setting or company to their private listing(s). We do not encourage parents or carers as friends on social networking platforms. It is appreciated that some staff might have close friends or relatives who have children attending the setting and therefore might have them as friends on their profile.
- Our staff and volunteers do not access their own personal social networking accounts during working hours or on the settings machines.
- No videos or photographs of the premises (inside and outside) should be taken or used on any social networking platforms without a director's permission.

- No videos or photographs of any registered children should be taken or used on any social networking platforms without a director's (or managers) and parent's permission.
- No videos or photographs of any staff or volunteers in uniform should be used on any social networking platforms.
- Our staff and volunteers do not conduct themselves in a way that is detrimental to the early years setting.
- Our staff and volunteers are aware that any inappropriate images on their personal sites may place your professional persona in jeopardy.
- We advise all to take care not to allow interactions on these social networking platforms to damage working relationships between employees and clients of the setting or company.
- Parents and carers can leave reviews about the setting on the social networking platforms which are setup and monitored by the company. Any slander or derogatory comments will be taken down and investigated and if necessary person(s) blocked.
- Parents and carers cannot upload or post their own media content (*for example: promotion, album, videos or photographs etc…*) to any social networking platform(s). The settings manager and director(s) are responsible for which content is displayed and/ marketed.
- Parents, carers and visitors can *'join'* or '*request to join'* a registered approved group or site associated with the company.

Cyber bullying
The setting is committed to ensuring that all of its staff are treated with dignity and respect at work. Bullying and harassment of any kind will not be tolerated in the workplace. The setting can provide clear guidance on how bullying and harassment can be recognised.

Cyber-bullying methods could include using text messages, mobile phone calls, instant messenger services, by circulating photos or video clips or by posting comments on web sites, blogs or in chat rooms. Personal blogs that refer to colleagues without their consent is also unacceptable. Staff who cyber-bully a colleague could also face criminal prosecution under various laws, including the Malicious Communications Act 1988.

Monitoring
The setting reserves the right, to monitor any and all aspects of its electronic resources. This includes: data, email and voice mail boxes, and other employer provided electronic storage systems. The setting also reserves the right for business and security purposes to audit and monitor the information on all systems, electronic mail, telephone and information stored on computer systems or media, without advance notice.

The setting also reserves the right to retrieve the contents of any employee communication in these systems. This process is in place to maintain the integrity of the setting's electronic systems, the rights of the other users, and to ensure compliance with the settings policies and obligations.

CCTV
Our settings are securely monitored by a CCTV surveillance systems. The Manager/Owner is responsible for the operation of the system for ensuring compliance with this policy.

The use of CCTV is a vital feature and used as a supportive management tool within childcare setting. CCTV operators have certain duties and responsibilities to those whose images are caught on camera. Our settings complies with the Information Commissioners CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use.

The use of CCTV and the associated images is covered by the Data Protection Act 1998. This policy outlines our use of CCTV and how it complies with the Act and is associated with the Data Protection policy, the provisions of which should always be adhered to.

Our system comprises of fixed position cameras, a monitor, digital hard drive recorder and public information sign(s). Cameras are located at strategic points on the premises. No camera is hidden from view and all will be prevented from focusing on areas of private accommodation such as toilets. Signs are prominently placed to inform staff, children, parents and visitor that a CCTV installation is in use. The digital recorder and single effectiveness of the limited system it is not possible to guarantee that the system will detect every incident taking place on the site.

Purpose of the System:
The system has been installed with the primary purpose to assist our management team monitoring:

- Staff interaction with children.
- Ensuring children are appropriately cared for.
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff and assist in providing evidence to the Manager.
- Reducing the threat of a child being abducted.
- Damaged to the building.
- Theft.
- Assist in the prevention and detection of crime.
- Helping ensure the safety of all the users, staff, children, parents and visitors, consistent with the respect for the individual's privacy.
- Deter those having criminal intent.

Recording
Digital recordings are made using a digital video recorder operating in real mode, monitoring the site continuously 24 hours a day. Images will normally be retained for between 5 to 7 days from the date of the recording and they will then automatically overwritten.

Access
Viewing of the recorded images of CCTV will be restricted to the Manager within the office, also to those staff who need to have access in accordance with the purpose of the system. Out of hours, the area manager, owners will have access to CCTV images via secure remote access to assist in maintaining the security of the premises. This is not a "webcam" facility; parents will not have access to view recordings.

Our system will not be used to provide images for the world-wide-web or record any sound. The setting and its contents is not used or shared with the public and/or clients. As a setting we must protect the identity of others (children/ adults) that potentially may be at risk.
Refusal to disclose images may be appropriate where the release would be likely to cause substantial and unwarranted upset, damage or said risk to that individual (child/ or adult).

Software or Programmes

- Software and/or programmes is purchased or licenced by the directors for the sole use of the setting(s).
- The purpose of using software and/or programmes is to:
- Access NIAB (Nursery in a box software):
  (ie: Staff & Children's Records, Registers & Occupancy Details, Fees & Invoicing, Child & Group Observations, EYFS profile, Monthly Reports, Cohorts, Holiday & Sickness, Timesheets, Employee Employment Details)

- Our staff use software and/or programmes to record, support, update, review and assess. Data from these are stored on the tablets and on the secure management suites.
- Staff and volunteers must not introduce or use their own software and/or programmes. Staff cannot change company platforms or systems without consulting and obtaining the approval of a director. Software and/or programmes are standardised and consistent intentionally throughout the businesses.
- Staff and volunteers must access support or training if they are unfamiliar with how to use software and/or programmes. However, staff must show a willingness to learn.
- Staff must not share passwords or access to our systems. These may include but not limited to: the Staff Portal, NIAB or any web Management Suite (emails, OneDrive or Microsoft Teams) from outside the setting (*unless authorised to do so, for example: manager network meeting*). Data is available on the Web Management Suite only to users within the setting with the appropriate password.
- Software and/or programmes must be used in a safe and appropriate manner, and any staff or volunteers found to be mistreating, purposely deleting or damaging data stored may result in disciplinary action.
- Observations and assessments may be emailed to parents, in which case the parent will have given their permission and the email address that they would like it to be sent to.
- Software and/or programmes need to be suitable for the age groups. Children are not to download, upload or be unsupervised.
- Staff must not use their own personal devices to access software of programmes owned by the business.

Staff and volunteers found to be in breach of this policy will be subject to an investigation which may lead to disciplinary action. Employees who breach this policy could also face criminal prosecution under various laws.