Safeguarding and Welfare Requirement: Child Protection

The safeguarding policy and procedures must include an explanation of the action to be taken in the event of an allegation being made against a member of staff, and cover the use of mobile phones and cameras in the setting.

1.5 Online safety (inc. Acceptable use of ICT, mobile phones and cameras)

Introduction

The internet should be considered part of everyday life with children and young people seen to be at the forefront of this online generation. Knowledge and experience of information and communication technology (ICT) should be considered an essential life skill. Developmentally appropriate access to computers and the internet in the early years will significantly contribute to children and young people's enjoyment of learning and development.

Children and young people will learn most effectively where they are given managed access to computers and control of their own learning experiences, however such use carries an element of risk. Early Years practitioners and managers, in partnership with parents and carers, should consider it their duty to make children and young people aware of the potential risks associated with online technologies. This will empower then with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

Policy statement

We take steps to ensure that there are effective procedures in place to protect children, young people and vulnerable adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting.

The policy applies to all individuals who are to have access to or be users of work related ICT systems. This will include children and young people, parents and carers, early years managers and practitioners, volunteers, students, committee members, visitors and contractors. This list is not to be considered exhaustive.

This policy will apply to internet access through any medium, for example computers, mobile phones, tablets and gaming machines. Before the use of any new technologies they will be examined to determine potential learning and development opportunities. Their use will be risk assessed before considering whether they are appropriate for use by children and young people.

Responsibilities

The Designated Lead Practitioner for Safeguarding (DLP) is to be responsible for online safety and will manage the implementation of this policy. In our setting the DLP is Sally Bowd (Centre Manager).

The Designated Lead Practitioner for Safeguarding will ensure:

- Day to day responsibility for online safety issues and will have a leading role in implementing, monitoring and reviewing this Policy.
- All ICT users are made aware of the procedures that must be followed should a potentially unsafe or inappropriate online incident take place.
- Recording, reporting, monitoring and filing of reports should a potentially unsafe or inappropriate online incident occur. This must include the creation of an incident log to be used to inform future online safety practice.
- All necessary actions are taken to minimise the risk of any identified unsafe or inappropriate online incidents reoccurring.
- Regular meetings take place with the registered person and/or managers to discuss current issues and review incident reports.
- Effective training and online safety advice is delivered and available to all early years managers and practitioners, including advisory support to children, young people, parents and carers as necessary.
- Liaison, where appropriate, with other agencies in respect of current online safety practices and the reporting and management of significant incidents.

Procedures

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to the setting is used by staff and children.
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- All computers have virus protection installed.
- The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.

Acceptable use by early years practitioners

- Early years practitioners a should be enabled to use work-based online technologies:
    - to record children's progress and development;
    - to access age appropriate resources for children;
    - for research and information purposes;
    - for study support.

- All early years practitioners will be subject to authorised use as agreed by the Centre Manager.
- All computers and related equipment are to be locked when unattended to prevent unauthorised access.
- All early years practitioners are to be provided with a copy of an Acceptable Use Agreement which they must sign, date and return, and will be kept on file.
- The use of personal technologies will be subject to the authorisation of the Centre Manager, and such use will be open to scrutiny, monitoring and review.

Acceptable use by children and young people

- Acceptable Use Agreements are to be used to inform children of the appropriate behaviours expected to ensure online safety. Children will also be informed of the behaviours which will be deemed unacceptable as well as encouraging them to tell a familiar adult about any access of inappropriate content, material that makes them feel uncomfortable or contact made with someone they do not know, straight away, without fear of reprimand. This will allow children to take some degree of responsibility for their own actions.
- In understanding Acceptable Use Agreements, children will become aware of the potential risks associated with misuse and the sanctions which will be applied, where necessary.
- The Acceptable Use Agreements are shared and agreed with children and will be displayed as a reminder.

Acceptable use by parents and carers

- Partnership working with parents and carers should be considered essential practice for promoting an agreed and consistent message which will define acceptable and unacceptable behaviours. Parents and carers will therefore be asked to sign an Acceptable Use Agreement together with their child in order to promote this shared message.
- Parents and carers are to be encouraged to contribute to the Acceptable Use Agreement and should be encouraged to use it should their child access similar technologies at home.
- Parents must only use photographs on/in children's learning journals for personal use and are not permitted to upload them to other websites or social networking sites.
- The use of personal technologies is not normally permitted within the setting. (see mobile phones below).

Managing online access

Password security

- Maintaining password security is an essential requirement for early years managers and practitioners particularly where they are to have access to sensitive information. A list of all authorised ICT users and their level of access is to be maintained and access to sensitive and personal data is to be restricted.
- Early years managers and practitioners are responsible for keeping their passwords secure and must ensure they are updated once every 60 days. All users must have strong passwords, for example a combination of numbers, symbols and lower and upper case letters.
- Sharing passwords is not considered to be secure practice. Where children and young people are to be enabled to create their own password a copy of such will be kept on file for reference.
- All computers and laptops should be set to 'timeout' the current user session should they become idle for an identified period.
- All ICT users must 'log out' of their accounts should they need to leave a computer unattended.
- If ICT users become aware that password security has been compromised or shared, either intentionally or unintentionally, the concern must be reported to the Designated Person for Safeguarding.

Internet access

- Children do not normally have access to the internet and never have unsupervised access.
- If staff access the internet with children for the purposes of promoting their learning, written permission is gained from parents who are shown this policy.
- The designated person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.
- Children are 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
  - 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
- Designated persons 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.
- If a second hand computer is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it.
- All computers for use by children are located in an area clearly visible to staff.
- Should children, young people or adults discover potentially unsafe or inappropriate material, they must hide the content from view. For example, the window will minimised and/or the monitor (not Computer) will be turned off. All such incidents must be reported to the DLP who must ensure a report of the incident is made and take any further actions necessary.
- Should it be necessary to download unknown files or programmes from the internet to any work related system it will only be actioned by authorised ICT users with permission from the Designated Lead Practitioner for Safeguarding (DLP). Such use will be effectively managed and monitored.
- 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.
- 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.
- The designated person ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.
- 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.

Online communications

- All official communications must occur through secure filtered email accounts.
- All email correspondence will be subject to scrutiny and monitoring.

- All ICT users are expected to write online communications in a professional, polite, respectful and non-abusive manner. The use of emoticons is not permitted.
- A filtered internet server is used to monitor and prevent offensive material or spam. Should, on occasions, security systems not be able to identify and remove such materials the incident will be reported to the Designated Person for Safeguarding immediately.
- Communications between children and adults by whatever method should take place within clear and explicit professional boundaries. Early years managers and practitioners will not share any personal information with any child or young person associated with the setting. They will not request or respond to any personal information from the child or young person other than which might be considered appropriate as part of their professional role. Advice should be sought from the DPS before engaging in any such communication.
- Early years managers and practitioners must ensure that all communications are transparent and open to scrutiny
- All ICT users should refrain from opening emails where they do not know the sender or where the content or format looks suspicious.
- Online communication is not considered private or confidential for safeguarding and security purposes. All users must seek advice from the DPS and the local Safeguarding Children Board as to how information should be relayed.
- Children and young people will be enabled to use online equipment and resources when it is considered, in consultation with parents and carers, that they have the developmental knowledge and understanding to recognise some of the benefits and risks of such communication. Access to online communication will always be supervised by an adult.
- When children and young people access online communications and communities a nickname must be adopted to protect their identity and ensure anonymity.

Managing multimedia technologies

- Many devices are equipped with internet access, GPS, cameras and video and audio recording functions. A risk assessment is completed to minimise risk of using technologies whilst maximising the opportunities for children and young people to access such resources.
- All ICT users and the DPS must only use moderated sites to afford maximum protection. Non-moderated websites allow for content to be added and removed by others.
- Children and young people, and their parents will not be permitted to post images taken on behalf of or at our setting on any website or profile.
- Staff maybe permitted to post images taken at the setting for specific purposes e.g. on the setting website to advertise our activities, however explicit consent will be required for this (see our image use policy).

Mobile phones – children

- Children are not permitted to bring mobile phones or other ICT devices with them to the setting. If a child is found to have a mobile phone or ICT device with them, this is removed and stored in the lockers in the office (Greenfield site) or in the locked filing cabinet (St Michaels site) until the parent collects them at the end of the session.

Mobile phones – staff and visitors

- Personal mobile phones are not used by our staff on the premises during working hours. They will be stored in lockers in the office (Greenfield site) or a locked drawer of the filing cabinet (St Michaels site).
- In an emergency, personal mobile phones may be used in an area where there are no children present, with permission from the manager.
- Our staff and volunteers ensure that the setting telephone number is known to family and other people who may need to contact them in an emergency.
- If our members of staff or volunteers take their mobile phones on outings, for use in case of an emergency, they must not make or receive personal calls, or take photographs of children. Staff are made aware that the manager will monitor/inspect personal phones to ensure that this is the case.
- Parents and visitors are requested not to use their mobile phones whilst on the premises, they will be asked to store them in the lockers in the office (Greenfield site) or a locked drawer of the filing cabinet (St Michaels site). We make an exception if a visitor's company or organisation operates a lone working policy that requires contact with their office periodically throughout the day. In this instance visitors will be advised of a quiet space where they can use their mobile phone, where no children are present.
- These rules also apply to the use of work-issued mobiles, and when visiting or supporting staff in other settings.

Cameras and videos

- Our staff and volunteers are not permitted to bring their personal cameras or video recording equipment into the setting.
- Photographs and recordings of children are only taken for valid reasons i.e. to record their learning and development, or for displays within the setting, with written consent received by parents (see the Registration form). Such use is monitored by the manager.
- Where parents request permission to photograph or record their own children at special events, general permission is gained from all parents for their children to be included. Parents are advised that they do not have a right to photograph anyone else's child or to upload photos of anyone else's children.
- If photographs of children are used for publicity purposes, parental consent must be received and safeguarding risks minimised, for example, ensuring children cannot be identified by name or through being photographed in a sweatshirt with the name of their setting on it.
- Consent must be obtained from parents and carers should their child be photographed amongst a group of children; and where consideration is to be given to including that image in a

learning journey belonging to another child. It will be anticipated that this will be a regular occurrence, as group activity shots are to be encouraged.

- Where possible, therefore, 'blanket' consent will be requested from parents and carers for group images to be included in the learning journeys of other children. Parents and carers will also be permitted to restrict their consent.
- All staff have a duty to report any concerns relating to potential misuse. Clear whistle-blowing procedures are in place to support this. An anonymous reporting system will also be promoted and used to facilitate this process.

Social networking sites

- Access to social networking sites is not usually permitted by children and young people in the setting. The manager or a person that they designate may access the settings social media sites/pages to maintain information for publicity purposes. This work will be monitored by the manager.
- Early years managers and practitioners are not permitted to use work related technologies for personal access to networking sites.
- The use of these sites in adults recreational time cannot be restricted however early years managers and practitioners must adhere to our professional conduct agreement. Content which may compromise professional integrity or will bring the setting into disrepute is not permissible and may result in disciplinary action.
- It is not permissible for early years managers or practitioners to engage in personal online communications with children, young people, parents or carers. This includes the use of social media networking platforms such as Facebook and Twitter.
- Any known misuse, negative and/or anti-social practices must be reported immediately to the DLP.
- If a practitioner and family are friendly prior to the child coming into the setting, this information is shared with the manager prior to a child attending and a risk assessment and agreement in relation to boundaries is agreed.

Online record keeping systems

- We use two online systems to process children's data. 'Tapestry' is an online learning journal system used to record your child's learning and development, and babysdays is an online system used to manage the administration of the setting e.g. room registers and invoicing. Both uk based, databases are completely secure, and unique to us. All information is accessed through a password system only. Information on learning journals is not stored on the setting computers or tablets.
- Access to information stored both databases can only be gained by unique user id and password, which is set up with parental consent when a child is registered with the setting.
- Parents can only see their own child's information.
- Staff use tablets to take the photographs for observations but these will not be stored on the device. Photos will be uploaded to the relevant database as they are taken and then deleted from the device.
- Staff access to both systems is secured by a unique user id and password which they must not share with anyone else.

- Entries to both systems are frequently moderated by the Centre Manager.
- Parents are asked to sign a consent form giving permission for their child's image to appear in other children's Learning Journeys, and to protect images of other children that may appear in any photos contained in their child's Learning Journey.
- In all written observations, other children are referred to by an initial and not by name. An exception to this may be where siblings are present in the same photograph.
- Staff only access tapestry on a preschool device, during preschool hours, and are given time away from the children each week to update children's records and make assessments.
- For parents without access to the internet; we will print all the information from Tapestry and put it into a folder. This will be in setting for the parent to view at all times and will be sent home three times a year.
- When the children leave the setting permanently, we will save the learning journey to disc for them, so they have a lasting record of their child's time at pre-school.
- Where a primary school also has Tapestry we will, with parental consent, transfer the child's learning journal to the receiving school's Tapestry database according to the directions provided on the Tapestry website.

Use and/or distribution of inappropriate images

- Staff are aware that it is an offence to distribute indecent images. In the event of a concern that a colleague or other person is behaving inappropriately, the Safeguarding Children and Child Protection policy, in relation to allegations against staff and/or responding to suspicions of abuse, is followed
- Staff are aware that grooming children and young people on line is an offence in its own right and concerns about a colleague's or others' behaviour are reported (as above).

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/

This policy was adopted by	Winterbourne Early Years Centre	*(name of provider)*
On		*(date)*
Date to be reviewed		*(date)*
Signed on behalf of the provider		
Name of signatory		
Role of signatory (e.g. chair, director or owner)		