ONLINE SAFETY AND INFORMATION STORAGE DEVICES POLICY

Online safety (or e-Safety) relates to the specific challenges and risks presented by new technologies, including the internet, mobile phones and other devices, for children and young people as well as adults, both within and outside of the setting. The term 'Information Storage Devices' refers to ALL information storage devices, including tablets, cameras, mobile telephones, and any recording devices such as smart phones and smart watches. We seek to create an appropriate balance between controlling access to the internet and technology, setting rules and boundaries and promoting awareness to children, parents/carers and staff about safe and responsible use. This will include a range of practices including undertaking appropriate risk assessments of technology, setting appropriate filters on ICT equipment, ensuring there is appropriate supervision of children, providing safe and suitable equipment/tools for staff and children and ensuring that there is up-to-date training/education in place for all staff, and support for parents regarding online risks and responsibilities. We are aware that children and staff cannot always be prevented from being exposed to online risks and will therefore seek to empower and educate all staff and parents/carers so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns.

All members of staff will be made aware of the importance of good online safety practice in order to educate and protect the children in their care. Members of staff will be made aware of the professional risks associated with the use of electronic communication (e-mail; mobile phones; texting; social network sites) and will be informed about how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role. Staff should familiarise themselves with advice and professional expectations outlined in 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' and 'Safer Practice with Technology – Guidance for Adults who Work with Children and Young People' (KSCB).

The Designated Safeguarding Leads (DSL), Janey Law and Leigh-Anne Osborne, are responsible for ensuring adequate training is given to staff, completing E-Safety Incident Logs when a concern is raised, and enforcing our E-safety procedures (see below).

PERSONAL MOBILE PHONES

- All mobile phones must be placed in the office in the nominated container, whilst staff, students, volunteers or visitors are directly with the children
- All mobile phones left in the office are done so at the owner's own risk. Clocktower Childcare accept no responsibility for theft, loss or damage to personal property left on the premises
- Staff are able to retrieve their mobile phone whilst on break in the staff area, office or off site
- The recording or sharing of images, video clips or audio material on any mobile phone is prohibited
- All mobile phone use is open to scrutiny and the Designated Safeguarding Lead may consider withdrawing or restricting use at any time
- In an emergency, Management may allow the use of a mobile phone to contact a parent/carer

SETTING MOBILE PHONE

- The setting mobile phone is essential when taking children offsite, e.g. to access school facilities, or on trips and outings etc.
- In these circumstances only, a staff member may be permitted by Management on occasions to take a personal mobile phone as an emergency back up
- The setting mobile phone provides an alternative method for parents/carers to contact us if the landline is unavailable, and we do allow parents/carers to text it also

USE OF CAMERAS, TABLETS, PHOTOGRAPHS AND VIDEOS

- Cameras / tablets are one of the key ways that we record children's development and engage parents in children's learning
- Setting owned cameras / tablets are provided for staff use for this purpose. Personal cameras / tablets are not permitted on site
- We may use photographs of the children for other purposes, including advertising, social media, local press and our website. Parental consent is obtained via our Registration Form
- We never use an identifiable photo accompanied by a full name (unless specific permission has been sought from parents/carers i.e. a newspaper article)
- Photos are not to be taken of children in an unsuitable state of dress or whilst in toilet cubicles / changing areas
- A child's wish not to be photographed is always respected
- Parents/carers are asked for permission at events to take photos / video footage for private use. If all agree, then they are asked to refrain from sharing such material on social media
- The opportunity for parents/carers to take photos / video footage at events can be reserved by Management at any time
- Setting cameras / tablets are not taken off site (but may be used within the school boundary e.g. on the trim trail)
- Photographs and videos taken and stored on cameras / tablets are be held in accordance with GDPR and the Data Protection Act 1998
- All tablets are set up with 'child friendly' settings, and include appropriate filters, blocked content etc.
- We occasionally arrange for professional photograph companies to visit the setting, and provide the chance for parents/carers to purchase orders. Any such visitor follows normal procedures, and will never have unsupervised access with children. We only use reputable companies.

SOCIAL MEDIA

- We have a Facebook Business Page, which has proven to be a successful way of interacting and communicating with parents/carers
- Only Management has access to the running and monitoring of this
- Parents agree via our Registration Form that they will not electronically share , including via social media, any part of their child's Learning Journal

- Staff are strongly discouraged from personally 'befriending' parents/carers, or existing or past children, on social media. However, we accept this is sometimes unavoidable in situations where they may be relations or long standing friends. More information can be found in the Staff Handbook
- Personal use of social media will be discussed with staff during the induction process, and may be monitored by Management. Staff are advised to be aware of content (including photos) published online relating to them which may deem them to be unsuitable to work with children. We also strongly suggest that they attempt to make themselves untraceable for parents/carers e.g. use of a different name, unidentifiable 'profile' pictures etc. Staff should avoid linking themselves publicly as an employee of the company and are aware that usual procedures regarding confidentiality are applicable to online activity also
- Any material online relating to a staff member that may have a negative impact on the setting in any way, will result in disciplinary action and possible dismissal

USE OF INTERNET / ACCEPTABLE USE

- Internet access by all users can be monitored at any time
- Any computerised records are stored in line with the Data Protection Act 2018 and General Data Protection Regulation (GDPR)
- Up to date anti-virus and spyware programs are implemented and regularly updated on setting laptops
- Children's access to the internet is fully supervised on age appropriate, pre-checked websites, for suitable lengths of time
- Online safety should be discussed with children through general day to day practice
- We focus on communicating awareness of E-Safety to parents/carers, through our welcome pack and website
- Every responsible precaution is taken to ensure the safe use of the internet. We do acknowledge however, that it will be impossible to safeguard against every eventuality
- All ICT users are expected to write any online communication in a polite, professional and respectful manner
- Staff are able to use ICT equipment and online resources for the purposes of fulfilling their roles
- Emerging technologies are to be examined to determine potential learning and development opportunities. Their use is to be risk assessed before consideration will be given to enabling use by children

E-SAFETY – REPORTING TO THE CHILD EXPLOITATION AND ONLINE PROTECTION CENTRE (CEOP)

If we're worried a child is being groomed online (or sexually exploited or radicalised), and have followed usual in-house procedures where relevant (including completing an E-Safety Incident Log), we will then report our concerns to CEOP. We will always report if a child is, or has, been in contact with someone who is:

- Chatting online to a child about sex
- Asking them to do sexual things on a webcam
- Asking to meet if they've only met online
- Requesting sexual pictures
- Forcing them into sexual activity
- Making them feel unsafe
- Making them question their beliefs
- Demonstrating extremist views

CEOP is a command of the National Crime Agency and can investigate what is happening, with the assurance that the safety and well being of the child is paramount at all times. If we were concerned a child was in immediate danger, we would call 999. Details of reporting to CEOP can be found on our Safeguarding Board.

This policy was adopted at a meeting of Clocktower Childcare Ltd held on 30th August 2019. Latest date to be reviewed: 31st August 2020.

Signed on behalf of Clocktower Childcare Ltd:

J. Law	*S. Wingham*	*L. Baverstock*
Jane Law, Director	Sally Wingham, Director	Lara-Jane Baverstock, Director