The Play Den
27 Safeguarding and Welfare Requirements
INFORMATION AND COMMUNICATION TECHNOLOGY POLICY – STAFF

- At The Play Den, staff are required to adhere to strict guidelines on the use of ITC equipment as well as how they access confidential information. The setting aims to reduce the risk of confidential information being accessed by unauthorised persons **(Safety and Suitability of Premises, environment and equipment 3)**
  by:
- Setting equipment such as laptops and tablets are password protected and staff are required to change their passwords every 3 months
- Information is only stored for as long as is necessary and for the purpose for which is was intended.
- Folders are created on the setting's laptop for individual staff and children to facilite sending information and to ensure information not pertaining to others are sent to unauthorised recipients
- Breeches will be reported to the ICO
- The setting uses the domain @theplayden.co.uk when dealing with parents and other professionals to reduce the risk of unauthorised access to emails. Staff ONLY use these email addresses when managing any setting related work.
- Staff do not use mobile devices to access emails and only access such information using the full websites. Only the Managing Director is able to access this information on her phone that has face ID and password protected.
- Staff are required NOT to save passwords to ANY device, including work equipment and must input passwords every time.

- In instances where information is of a sensitive nature (such as safeguarding) the information is sent securely according to local authority guidelines. In all other instances, staff will use the initials of the child only.
- Only managers at The Play Den can upload images to the website or the setting Facebook page. Such media is password protected. Managers can also comment on events and activities. Parents/carers are able to leave comments however these are monitored for appropriateness before being displayed.
- When sending e-mails to a group or parents or parents, BCC will be used to ensure confidentiality of other families.
- Tablet devices and cameras are not permitted off site and are stored in the setting's (locked) office overnight.
- Staff are able to store 14 days of photographs only and photographs must be deleted by this time
- Staff are allowed to access emails from managers at home but must ensure when doing so, confidential information cannot be viewed by others (such as family members). Additionally, staff must use the full website browser (not apps) and never save the password.
- Only the WhatsApp page created by managers can be used to cascade information to each other and other 'groups' must not be created on any social media.
- Laptops, tables or phones that do not belong to the setting are prohibited and staff must not use personal laptops to process work information.
- Regular 'spot checks' will be conducted on work devices to monitor passwords and the use of sites.
- When using Tapestry, staff must ensure care is taken to ensure breeches of confidentiality do not occur. This is especially prudent when uploading multiple observation when staff must use the initials of children only.
- ITC equipment will be monitored on a monthly basis and the policy will be reviewed every 6 months
- It is a disciplinary offence for any staff member to breach the terms of this policy, particularly the use of accessing setting information outside of work. Breaches of confidentiality will be dealt with severely and may involve an investigation by the Information Commissioner (if the Data Protection Act has been breached) and parents may be informed.

- Staff will receive training in respect of 'The Prevent Duty' and must monitor children's behaviour for signs of radicalisation and ITC use for signs of extremist material.

This policy was produced on 3/12/15 and last updated on 13/4/19