Safeguarding and Welfare Requirement: Child Protection
Providers must have and implement a policy, and procedures, to safeguard children.

1.6 – E- Safety and the use of Mobile Phones, Recording and other Technological devices Policy

E-Safety

Data storage and management
No electronic documents that include children's names or digital images will be transported out of the setting e.g. on Fobs, memory sticks. **For more information on Transporting data please refer to Policy 10.11.**

Setting issued devices should not leave the premises unless encrypted. In the case of an outing, all data must be transferred/deleted from the setting's camera/device before leaving the setting. **Please see our Tapestry Policy 10.10** for more information on staff using tablets to complete each child's individual learning journey.

Policy 10.7 Provider records states;
"With the introduction of GDPR we have compiled Privacy notices for children and parents, staff , students as well as the committee. These outline how we use the personal data outlined above by stating; who has access to it, how it is stored, what the data is used for, length of time it is retained in the setting as well as how it will be destroyed. These notices can be found in the **Appendix section** along with Cambridgeshire county councils retention record periods for Early Years settings which supports how long we will keep data for within Witchford Rackham Pre-School."

Email
The setting has access to a professional email account to use for all work related business, including communication with parents/carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families.

Staff must not engage in any personal communications (i.e. via hotmail or yahoo accounts etc.) with children who they have a professional responsibility for. This also prohibits contact with children who previously attended the setting.
Staff should not participate in any material that is illegal, obscene and defamatory or that is intended to annoy or intimidate another person or persons.
All emails should stay professional in tone and checked carefully before sending, just as an official letter would be. Care should be taken when forwarding emails from others.

Social Networking

Employees must not access personal blogs/social networking sites on work premises or use the setting's internet systems or email address for their own use, without prior agreement or in accordance with the setting's policy.

The setting does not condone employees writing about their work on social networking sites or web pages. If employees choose to do so, they are expected to follow the rules below.

Staff must not:

- disclose any information that is confidential to the setting or any third party or disclose personal data or information about any individual child, colleague or service user, which could be in breach of the GDPR(2018) ,Data Protection Act 2018 and pre-schools **confidentiality policy (1.4).**
- disclose the name of the setting or allow it to be identified by any details at all. This includes posting photos of children and young people, the premises or events with work colleagues.
- link their own blogs/personal web pages to the setting's website.
- make defamatory remarks about the setting, colleagues or service users.
- misrepresent the setting by posting false or inaccurate statements.

Mobile Phones and Cameras and recording devices.

- Staff, visitors, volunteers and students are not permitted to use mobile phones to take or record any images of the children. Staff must only use the designated camera(s)or Tablet(s) whenever they are taking photographs in the setting. Parents need permission from the designated safeguarding practitioner to use cameras, videos or mobile phones for photographs, images or recording in the setting.
- We use an online system called Tapestry to record and store all observations and assessments relating to children. **Please refer to Policy 10.10 for further information about the safety and security of this.**

- Aside from photos and videos as observations we take photos of the children when they start at pre-school for self-registration, birthday board, key group board and for using the tablet. Staff will also take group observations which will be used to display on boards and parents will send via email or post photos on tapestry for the Pre-School manager to print and use as part of displays. These photos are stored in line with the GDPR (2018). Article 5 states "Personal Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures." The photos are only kept on the computer whilst the child is in attendance at the pre-school and therefore deleted appropriately and the Pre-School Manager and Deputy are the only ones which have the password to log in to the computer. All photos around the setting of the children are given to them when they leave the setting or are destroyed using a shredder and disposed of appropriately. **Please refer to Policy 10.7 Provider Records and Policy 10.11 Data Transporting procedures for further information about how we store and transport personal data.**

- Events such as, sports day, outings, Christmas and fundraising events may be recorded by video and photographs by staff and parent/carers but always in full view of all attending. Parents/carers, staff, volunteers and students will be notified of this in advance. At the beginning of every event parents/carers, staff, volunteers and students will be reminded not to include photographs of children other than their own on social media such as facebook.

- Mobile phones belonging to staff, volunteers, students and others should be switched off, signed in and placed within the designated basket which will be placed within the Managers office at the beginning of each session. Personal calls must be directed through the settings phone. Staff must not make personal calls during their working hours. However, in urgent cases, a call may be made or accepted if deemed necessary and by arrangement with the Manager.

- Any staff member or student wearing a smart watch will be asked to turn off all notifications to the smart watch before session starts to ensure they are not distracted from the duty of care they have for the children by their smart watch going off.

- Outside professionals who are coming to work within the setting can retain their, mobiles however are to be advised to take calls if needed within a quiet room away from the children. No outside professionals will be left unattended with children.

- Visitors and parents should only use their phones outside the building unless they have received permission from the designated officer. If they remain on the person whilst on site they must be switched off and remain out of sight. Should this not be complied with staff have the right to challenge and refer them to the setting safeguarding policy.

- Staff will be vigilant when children are in the outside area to prevent unauthorised persons taking photographs or recording images. Staff if they notice anyone doing so will ask the person to stop and report this to the Manager immediately.

Children's tablets

The tablets which the children have access to have separate profiles for adults and children. The manager controls the apps which are downloaded for the children to use within session time through the adult password protected profile on the tablet. Only the manager knows the password. The children do not have direct access to the internet on the devices.

This policy was adopted at a meeting of Witchford Rackham Pre-school

Held on _____

Date to be reviewed _____

Signed on behalf of the

Management Committee _____

Name of signatory _____

Role of signatory _____