Internet and use of personal devices

The setting's internet connection is provided by Melbourn Primary School.

The following rules apply:

- The internet can be freely accessed for setting matters (including finding resources, planning etc).
- Any information and digital images stored of children will be stored within the Dropbox or Tapestry systems. These are password protected and only accessible by relevant adults.
- Emails sent on behalf of the setting, particularly to parents, should be sent through the setting email accounts. No personal communication should be entered. This is to ensure the smooth running of the setting and protect staff and the reputation of the setting.
- Staff must be aware of their responsibilities to the setting when using the internet, including any social networking sites. Our confidentiality policy must be always adhered to, even outside of working hours. Staff members are obliged to follow normal reporting procedures if they acquire any information gained through social networking, which suggests a safeguarding issue. Friendships and/or connections via social media that exist prior to employment are accepted if the above is observed. It is an expectation of the setting that new friendships/social media connections will not be made with anyone connected with Melbourn Playgroup and Out of School Club apart from work colleagues. Disciplinary action could result if the setting is brought into disrepute. Once a family has left the setting these rules no longer apply.
- Staff and Parents must not put pictures of any of the children on the Internet without prior consent from the parents of all children concerned.
- Children are to be encouraged to use the internet if appropriate but must be supervised at all times.

Personal technological devices by staff, volunteers and visitors

Personal mobile phones must be stored in the box provided in the office and only may only be accessed during break times when staff are away from the children. Smart watches must be disabled from any internet functionality. Smart watches with a camera feature are not to be worn to the setting.

In exceptional circumstances, such as a family emergency, staff and volunteers should seek permission from the manager or employer to use their mobile phone.

If a staff member, student or volunteer must use their mobile phone (see above) this should be away from the children and ensuring that staff supervision levels are not compromised.
Consideration will be given to staff or children who have a technological device to record medical needs such in the case of recording blood sugar levels. This will be risk assessed recognising the unique need of this device and the clear use of it for the individual.
The setting's main telephone number can be used for emergencies by staff or volunteers or by people who need to contact them.
In circumstances such as outings and off-site visits, staff will agree with their manager the appropriate use of personal mobile phones in the event of an emergency.
Staff, students, volunteers and visitors remain responsible for their own property and will bear the responsibility of any losses.
Visitors will not use mobile devices near the children.

Use of the setting's technological devices

Only technological devices belonging to the setting may be used to take appropriate and relevant images of children.
Images must be used in accordance with the Data Protection Act 2018.
Technological devices should only be used where two or more staff members are present.
It is **not** appropriate to take photographs of bruising or injuries on a child for child protection concerns. The 'Logging Concern Form and Body Map' must be used to record factual observations.
The setting's mobile phone must only be used for work related matters.
The setting's technological devices remain the property of the setting at all times and should not be taken off of the premises (with the exception of visits and outings).

Social Media

- Staff must always act in the best interests of the setting.
- Staff should observe confidentiality by not discussing children, parents or other practitioners when using social media.
- Staff should not post any photos of children on their social media sites unless they are already known to them in a personal capacity and the photos are not connected or related to the setting in any way.
- Staff must not accept children, parents or carers as "friends" on social media.

If a staff member is already friends with a parent/carer before the child starts at the setting (as they already know them in a personal capacity) they must not discuss or share any setting related information on social media sites with them.

- Staff members are obliged to follow the normal reporting procedures if they acquire any information gained through social networking, which suggests a safeguarding issue.
- When using social media staff should always consider how their social conduct may be perceived by others and how this could affect their professional reputation and that of the setting.
- Disciplinary action will be taken if there is a breach of confidentiality or defamatory remarks are made against the setting by any staff member.