‘e’ SAFETY POLICY

Statement of intent
Little Acorns recognises its duty to ensure that children are protected from potential harm. All staff have a shared responsibility to ensure that children can use the internet and related technologies appropriately and safely as part of the wider duty of care to which all adults working with children are bound.

Internet abuse is any type of abuse that happens on the web, whether through social networks, playing online games or using mobile phones, such as cyberbullying, grooming, sexual abuse, sexual exploitation, exposure to pornographic images or emotional abuse.

Aim
Little Acorns aims to ensure that children stay safe and secure when using the internet and/or related technologies by:

- Raising awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many educational and social benefits
- To provide safeguards and rules for acceptable use to guide all users in their online experiences
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond Little Acorns.

Methods
The use of the internet and related technologies enables Little Acorns not only to communicate with parents and carers but also to have access to a wealth of resources and support.
Little Acorns uses tablets, iPads, educational apps and games to enhance the learning experience of children and as an online tool for staff to track and share achievement with parents/carers.

Procedure
- The named person with overall responsibility for ‘e’ safety is Val Duffy, they are required to keep themselves up to date with legislation and research and to ensure that all staff have relevant training and support in order to maintain the security of the network and safeguard children.
- Little Acorns ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Anti-virus software is installed and maintained on all setting machines and portable devices.
- Filtering is applied and updated on a regular basis. The member of staff with the responsibility for ‘e’ safety will allow or block access to sites and manage user internet access. The Designated Person for Safeguarding will monitor this.
- Age appropriate content filtering is in place across the setting, ensuring that staff and children receive different levels of filtered internet access in line with user requirements.
- Any changes to filtering levels are documented and include the reason for the requested change, the date and name of staff member concerned.
- Any problems or faults relating to filtering are reported to Designated Person for Safeguarding and to the broadband provider immediately and recorded on the ‘e’ Safety Incident Log.
- Users may only access Little Acorns network through a rigorously enforced password protection policy, in which passwords are regularly changed. Staff should keep their passwords confidential and not allow unauthorised access to equipment.
- The use of the setting’s network is regularly monitored in order that any deliberate or accidental misuse can be reported to the ‘e’ safety lead and Designated Person for Safeguarding.

- Personal staff mobile phones or devices (e.g., iPad or iPhone) will not be used for any apps which record and store children's personal details, attainment, or photographs. Only Little Acorns issued devices will be used for such activities, ensuring that such devices are used appropriately and encrypted. If such devices are taken off site, this is done with prior agreement with Val Duffy and reasons for this recorded.
- Children's data will be stored securely.
- The setting provides all staff with access to a professional email account to use for all work related business, including communication with parents and 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.

Social Networking

Little Acorns recognises that social networking sites (e.g. Facebook and Twitter) can be a useful advertising tool and an effective way of engaging with parents/carers. Due to the public nature of social networking and the inability to keep content truly private, great care will be taken in the management and use of such sites

- Identifiable images of children will not be used on social networking sites.
- To maintain professionalism, staff should not link their personal social networking accounts to the setting's page.
- Privacy settings will be set to maximum and checked regularly.

Children's Use:

Internet and related technology use will be always supervised by an adult and any games or apps used must be from a pre-approved selection checked and agreed by the Manager and Safeguarding Officer.

- Online searching and installing/downloading of new programmes and applications is restricted to authorised staff members only. Children will not be allowed to search or install anything on a setting device.
- Parental controls are established on all internet enabled devices that children have access to, blocking or preventing access to any harmful, illegal, or inappropriate content.

Parents/Carers

Little Acorns will offer support to parents/carers to enable them to provide a safe 'e' environment at home. This will include signposting to web sites such as NSPCC and CEOP.

Conduct

All staff working at Little Acorns are expected to maintain high standards of conduct and behaviour both within and outside of their professional responsibilities. Their roles and responsibilities which require them to work with children, young people and their families, some of whom may be vulnerable or at risk, carries a duty of care and places staff in a position of power and trust. For this reason, staff should carefully consider their personal use of social networking sites and review not only the level of private information that they share online but also the suitability of any content in respect of their professional role. All communications should acknowledge and maintain respectful professional boundaries and be transparent and open to scrutiny.

Any situations where a staff member feels they, or a user, may have compromised their professionalism should be reported to the Manager or Deputy Manager immediately.

If it is suspected that a member of staff has misused social networking in an abusive or illegal manner, a report must be made to the Manager or Deputy Manager, Little Acorn's Safeguarding Officer and Little Acorns Safeguarding and Staff Conduct Policies and Procedures followed.

If proven, any inappropriate behaviour by a member of staff will be the subject of a disciplinary process and, if necessary, a criminal investigation which could result in the individual being barred from working with children and young people