18. E-SAFETY POLICY

Policy Statement

All early years settings have a duty to ensure that children are protected from potential harm within and beyond the learning environment.

Aims

To raise awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many educational and social benefits.

To ensure adults are clear about procedures for misuse of any technologies both within and beyond the early years setting.

This policy applies to all staff, children, parents/carers, committees, visitors and contractors accessing the internet or using technological devices on the premises. This includes the use of personal devices by all of the above mentioned groups, such as mobile phones or iPads/tablets which are brought into Playgroup.

Staff Responsibilities - Practitioners (including volunteers)

All staff have a shared responsibility to ensure that children are able to 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. Anti-virus software is installed and maintained on all setting machines and portable devices. All Playgroup computers, tablets and internet connection are password protected.

Email Use – Staff

Staff must not engage in any personal communications (i.e. via Hotmail or yahoo accounts etc) with parents/carers of children who they have a professional responsibility for.

Mobile/smart phones

Staff:

Personal mobile phones are permitted on setting grounds, but are to be used during break times only, within designated areas away from children.

Personal mobile phones must never be used to contact children's families, nor should they be used to take videos or photographs of children.

Photographs and Video

Digital photographs and videos are an important part of the learning experience in early years settings and, as such, staff have a responsibility to ensure that they not only educate children about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and children about the use of digital imagery and videos.

- Written consent must be obtained from parents or carers before photographs or videos of young people will be taken or used within the setting, including displays, learning journeys, setting website and other marketing materials.
- Staff will ensure that children are at ease and comfortable with images and videos being taken.
- Staff must not upload photographs or videos from Playgroup equipment to their own personal social networking sites.
- Staff must not use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of children. However, in exceptional circumstances, such as equipment shortages, permission may be granted by the Provider/Manager for use of personal equipment for setting related photographs or videos, provided that the there is an agreed timescale for transfer and deletion of the image from the staff member's device.
- Setting issued devices only should be used for this purpose and, if containing sensitive information or photographs of children, 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.

Laptops/iPads/Tablets
Staff use

- Staff will ensure that setting laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.
- Setting issued devices only should be used for this purpose and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted and this must be acknowledged in the policy.

Applications (Apps) for recording pupil progress

- **Personal staff mobile phones or devices (e.g. iPad or iPhone) should not be used for any apps which record and store children's personal details, attainment or photographs. Only setting issued devices may be used for such activities, ensuring that any devices used are appropriately encrypted if taken off site. This is to prevent a data security breach in the event of loss or theft**.

Data Storage and Security

- Sensitive data, photographs and videos of children are not stored on setting devices which leave the premises (e.g. laptops, mobile phones, iPads, USB Memory Sticks etc) unless encryption software is in place.

Incident reporting

Please report any incidents to Sue Panther or Wendy Modeste – Safeguarding officers

PLAYLEADER SIGNATURE.....DATED.....

COMMITTEE SIGNATURE.....DATED.....

Royston-policy-e-safety-2023

Further information

Think U Know: www.thinkuknow.co.uk

Childnet: www.childnet.com

Safe: www.digitalme.co.uk/safe