1.10 Online Safety Policy

Policy Statement

Little Gillies take steps to ensure that there are effective procedures in place to protect children, young people and vulnerable adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials in the setting. Every effort will be made to safeguard against all risks, however it is likely that we will never be able to completely eliminate them. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children and staff continue to be protected.

This Policy is part of Little Gillies E Safety Policies and applies to staff, students, board members and volunteers of Little Gillies and should be read in conjunction with the following Policies: Social Networking Policy, Use of Image Recording Device Policy, Mobile Phone Policy and Tapestry Policy.

The Aim of the Policy

- To offer valuable guidance and resources to staff to ensure that they can provide a safe and secure online environment for all children in their care
- To raise awareness amongst staff and parents/carers of the potential risks associated with online technologies
- 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 Gillies

Procedures

- Our designated persons responsible for co-ordinating action taken to protect children are:
  Manager Sarah Beresford
  Deputy Manager Rachel Williams

- 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.

Information Communication Technology (ICT) equipment

- Only ICT equipment belonging to Little Gillies is used by staff and children.
- The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
- All computers, lap tops and tablets have virus protection installed.

- All computers, lap tops and tablets are password protected. The passwords are only known to Little Gillies staff and changed whenever staff leave.
- The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.
- If a second hand computer is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it.
- Staff are aware that all activities carried out on Little Gillies devices and systems, both within and outside of the work environment, will be monitored in accordance with this policy
- Staff will ensure that Little Gillies laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing

Internet access

- Children do not normally have access to the internet and never have unsupervised access.
- If staff access the internet with children for the purposes of promoting their learning, written permission is gained from parents who are shown this policy.
- The designated person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.
- Laptops, computers and tablets use must be supervised by an adult at all times and any games or apps used must be from a pre-approved selection checked and agreed by the designated person
- Online searching and installing/downloading of new programmes and applications is restricted to the manager, deputy manager and room managers only. Children should not be able to search or install anything on a setting device.
- Children are taught the following stay safe principles in an age appropriate way prior to using the internet;
    - only go on line with a grown up
    - be kind on line
    - keep information about me safely
    - only press buttons on the internet to things I understand
    - tell a grown up if something makes me unhappy on the internet
- Key persons will also seek to build children's resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age appropriate ways.
- All computers for use by children are located in an area clearly visible to staff.
- Children are not allowed to access social networking sites.

- Staff will report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.

- Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk.
- The designated person ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.
- If staff become aware that a child is the victim of cyber-bullying, they discuss this with their parents and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk.

Email

- Children are not permitted to use email in the setting. Parents and staff are not permitted to use setting equipment to access personal emails.
- Staff do not access personal or work email whilst supervising children.
- Managers can access their work email but only at an appropriate time
- Staff do not send personal information by email and share information securely at all times.
- All emails should be professional in tone and checked carefully before sending, just as an official letter would be
- Email is covered by the Data Protection Act (1988) and the Freedom of information Act (2000) so safe practise should be followed in respect of record keeping and security.
- All staff is aware that all email communications may be monitored at any time in accordance with the Acceptable Use Policy.
- All users must report immediately any email that makes them feel uncomfortable, is offensive, threating or bullying in nature.

Data Storage and Security

- In line with the requirements of the Data Protection Act (1988), sensitive or personal data is recorded, processed, transferred and made available for access at Little Gillies.
- This data must be accurate; secure; fairly and lawfully process; processed for limited purposes and in accordance with the data subjects rights; adequate, relevant and not excessive; kept no longer than necessary; and only transferred to others with adequate protection.
- At Little Gillies we specify how we keep data secure and inform staff as to what they can/cannot do with regard to data through this E Safety policy.
- Staff should not share their passwords with anyone; write their passwords down or save passwords in web browsers if offered to do so.
- Staff should not use their username as a password.
- Staff should not email their password or share it in an instant message.
- Staff should change their password if they think someone may have found out what it is.
- Staff should be aware of who they are allowed to share information with. Clarification can be obtained from the designated person.

- The use of unencrypted memory storage devices to store information of a personal sensitive or confidential nature is not permitted.
- Staff should only download files or programs from trusted sources. If in doubt, advice should be sought from the designated person
- Staff should lock sensitive information away when left unattended.
- Unauthorised people should not be allowed into staff areas.
- Computer screens should be positioned so that they cannot be read by others who shouldn't have access to that information.
- Confidential documents should not be left out.
- Staff should only take information offsite when authorised and only when necessary.
- On occasions when this is necessary, staff should ensure that the information is protected offsite in the ways referred to above.
- Staff should be aware of their location and take appropriate action to reduce the risk of theft.
- Staff should ensure that they sign out completely from any services they have used, for example email accounts.
- Staff should try to reduce the risk of people looking at what they are working with.

Serious Incidents

- If a serious incident occurs such as inappropriate content is accessed, the E safety incident log is completed immediately.
- The designated person is informed and the use of the ICT device suspended until it has been ensured that the pathway is blocked.

Useful Links and Further Guidance

Data protection and Freedom of information act: www.ico.org.uk
NSPCC – Keeping Children Safe Online www.nspcc.org.uk

Other Little Gillies policies and procedures that staff and parents/carers should have particular regard to include:

- Social Networking Policy,
- Use of Image Recording Device Policy
- Mobile Phone Policy
- Tapestry Policy
- Confidentiality Policy
- Safeguarding Policy
- Information Sharing Policy
- Staff Code of Conduct
- Staff Disciplinary Procedures

Any member of staff who fails to comply with this policy will be in breach of their terms and conditions of employment. This may result in disciplinary action in line with Little Gillies Disciplinary Procedures being taken and their Contract of Employment may be terminated.

All policies and procedures are implemented, reviewed and updated on an annual basis or in line with any changes to local and national guidance/legislation in conjunction with the registered person.

This policy was adopted at a meeting of Little gillies

Held on……

Date to reviewed ……

Signed on behalf of the provider……..

Name of signatory……..

Role of signatory……..

Reviewed by Sarah Beresford
Date June 2023