Play in Ltd

Internet Safety Policy

Play in Ltd recognises that the Internet is a useful resource for both staff and children, for purposes of research, homework and entertainment. However it must be used with care to ensure that children are kept safe from exposure to harmful material, in accordance with the EYFS safeguarding and welfare requirements and the Prevent Duty.

Children will only be allowed to access the Internet at the Club if their parent or carer has given written permission. A copy of the **SMART** guidelines will be printed out and kept next to the computer. The guidelines will be explained to any children wishing to access the Internet:

- **Safe:** Keep safe by not giving out personal information – such as name, email, phone number, address, or school name – to people who you don't trust online.
- **Meeting:** Never agree to meet anyone you have only met online unless your parent or carer is with you.
- **Accepting:** Do not accept emails or instant messages, or open files, images or texts from people you don't know. They can contain viruses or nasty messages.
- **Reliable:** Not all the information found on the Internet is reliable and people you meet online won't always be telling the truth.
- **Tell:** Tell a member of staff or your parents if someone or something you encounter online makes you feel uncomfortable.

At the current time, our club has no computers or club devices where the internet is accessible to children. Children's smart phones are to be kept in their bags or in the staff office if needed and are not to be used when at the club. However on occasion staff may access the internet to provide a service such as music or films as entertainment for the children. We have put in place the following safeguards for staff to be able to do this safely:

- A risk assessment has been undertaken
- The computer is located so that the screen can easily be seen from the rest of the room.
- Staff will supervise the use of the Internet
- The computer has an up to date virus checker and firewall installed
- Google SafeSearch Filtering is used; children are encouraged to use a child-safe search tool
- The computer's browser history is regularly checked to monitor which sites are being accessed and all staff and children are informed of this fact

However digital technologies have become part of the everyday lives of children and young people in today's society. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Children and young people, staff, volunteers and students have a right to safer internet access at all times. However, the use of these new technologies can put users at risk. The breadth of issues within online safeguarding is considerable, but they can be categorised into three areas of risk:-

Content: being exposed to illegal, inappropriate or harmful material
Contact: being subjected to harmful online interaction with other users
Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Play in LTD staff will also promote British values, staff at our setting will be alert to the fact that whilst extremism and radicalisation is broadly a safeguarding issue there may be some instances where a child or children may be at direct risk of harm or neglect from Extremism and Radicalisation. Therefore all adults working in our setting (including visiting staff, volunteers' contractors, and students on placement) are required to report instances where they believe a child may be at risk of harm from Extremism and Radicalisation to the DSL or setting Manager.

If, despite the above safeguards, a child encounters harmful material on the internet whilst at the club, receives inappropriate messages, experiences online bullying or accidentally viewing extremism material. The manager will be informed and the incident will be noted on an **Incident Record**, which the child's parent will need to sign. The manager will investigate how to prevent a reoccurrence of the incident.

If staff become aware that a child is deliberately attempting to access sites containing sexual, extremist or otherwise inappropriate material, or has been shown such material by a third party, they will complete a **Logging a concern form** and refer the matter to the Club's DSL, Niala Haq in accordance with our Safeguarding Children Policy.

Roles and Responsibilities

Safeguarding is considered everybody's business and online safety is not the sole responsibility of one individual. An agreed, shared approach must be promoted by all. The following section outlines the roles and responsibilities for the online safety of users within the Setting.

Management:

- The Owner and manager Niala Haq has the overall responsibility for ensuring the safety (including online safety) of all children and young people, staff, volunteers, students and members of the setting.
- The Owner/Manager and Deputy manager are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff or volunteer.
- The Owner/Manager is responsible for ensuring that the Online Safeguarding Lead Person and other relevant staff / volunteers/ students receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Owner/Manager will ensure that there is a system in place to allow for the monitoring of online safety in the Setting and that they receive regular monitoring reports.

Online Safeguarding Lead Person:

The online safeguarding Lead Person: Niala Haq

- Ensures that all staff / volunteers / students are informed of online safeguarding policies and procedures as part of the induction process and that access to information and systems are withdrawn on leaving the Setting's employment.
- Ensures that staff / volunteers / students have an up to date awareness of the Setting's current online safeguarding policy and practices.
- Ensures that children and young people are supported to learn about online safety in a way which is appropriate for their age and development.
- Ensures that all staff / volunteers / students are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies / documents

- Offers advice and support for all users
- Keeps up to date with developments in online safety
- Understands and knows where to obtain additional support and where to report issues
- Communicates with mothers and fathers/partners/carers
- Monitors incident logs
- Reports regularly to the Owner/Management Committee/Directors
- Ensures provision of training and advice for staff, volunteers and students
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Liaises with the national / local organisation / association as relevant

The Lead Person will be trained in online safety issues and be aware of the potential for serious child protection issues.

Staff:

They are responsible for ensuring that:

- They are aware of the type of abuse which can take place online.
- They are aware that safeguarding relates to broader aspects of care and education including the widening range of issues associated with technology and a user's access to content, contact with others and behavioural issues.
- They have an up to date awareness of the Setting's current online safety policy, guidelines and practices
- They have read, understood and signed the all relevant policies and risk assessments
- They report any suspected misuse or problem to the DSL (Niala Haq) – particularly where it is believed that a child's welfare is at risk.
- Digital communications with children and young people should be on a professional level and carried out using the official systems of the Setting.
- Children and young people in their care are aware of online safety
- All are aware of online safety issues and risks particularly those related to the use of mobile phones, tablets, i-pads, cameras, gaming consoles and hand held devices and that they monitor their use and implement the Setting's policies with regard to these devices.
- Staff promote how children can keep themselves safe from risks to develop the children's understanding of how to keep safe online.
- All are aware of the Setting's policy with regard to the use of mobile phones and cameras
- Staff oversee the safe use of technology when children are in their care and take action immediately if they are concerned about bullying or the child's wellbeing online.

Children and their families

- They need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Should demonstrate positive online behaviour
- Mothers and fathers / carers should be aware of and adhere to the Settings policies in relation to the use of mobile phones/personal devices and the taking of photographs/video images.

Supporting children and young people to stay safe online
Children and young people need help and support to recognise and avoid online safety risks and build their resilience. Online safety awareness will be provided in the following ways:

- Opportunities will be made to highlight online safety issues in relevant leaflets and posters for children, young people, mothers and fathers / partners/carers and staff, volunteers and students
- Online safety issues will be discussed / highlighted, when possible, in informal conversations with children and young people.
- When the opportunity arises, children and young people will be advised that not everything on the internet is true or accurate and that they should check that the materials / content they access on-line is from a reliable source and accurate.
- Young people should be made aware of the need to respect copyright when using material accessed on the internet and, if applicable, acknowledge the source of information used.
- Staff and volunteers should act as good role models.

Raising Awareness for mothers and fathers / carers
Many mothers and fathers / carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences. They often underestimate the extent to which children and young people are able to access the internet.

We will provide online safety information and awareness to mothers and fathers / partners/ carers through:

- Letters, newsletters, web site, notice boards
- Meetings with mothers and fathers / carers (formal and informal).
- Reference to the Sheffield Safeguarding website and other relevant resources.
- Sharing the Setting's policies with mothers and fathers / carers.

Training – employees
It is essential that all staff, volunteers and students receive online safety awareness training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All understand the risks posed by adults or peers who use technology, including the internet, to bully groom, radicalise or abuse children.
- A planned programme of training about online safety will be made available to staff, volunteers and students to keep their knowledge updated.
- All new staff, volunteers and students will receive awareness training as part of their induction programme, ensuring that they fully understand the setting's policies linking to online safety.
- An audit of the online safety training needs of all staff will be carried out regularly
- The online safeguarding Lead Person (Niala Haq) will receive regular updates by reviewing guidance documents released by the national organisation / SSCB / the local authority and others.
- The online safeguarding Lead Person (Niala Haq) will provide advice / guidance / training to individuals as required
- This online safeguarding policy and its updates will be presented to and discussed by staff, volunteers and students at staff / team meetings.

Protecting the professional identity of staff

This applies to any adult, but particularly those working with children and young people (paid or unpaid) within the Setting. Consideration should be given to how your online behaviour may affect your own safety and reputation and that of the Setting. Communication between adults and children by whatever method, should be transparent and take place within clear and explicit boundaries.

As a setting we do not use digital communications will our children, however staff must:

- Not share any personal information with a child or young person e.g. MUST NOT give their personal contact details to children and young people and their families including e-mail, home or mobile telephone numbers.
- Not request any personal information, or respond to requests to provide any personal information, from the child/young person. If you suspect a child is at immediate risk of harm you such inform the DSL (Niala Haq) instantly.
- Not send or accept a friend request from the child/young person on social networks.
- Be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised, e.g. Designated E-Safeguarding Lead Person
- Be careful in their communications with children/young people so as to avoid any possible misinterpretation.
- Ensure that if they have a personal social networking profile, details are not shared with children and young people in their care and their families (making every effort to keep personal and professional online lives separate).
- Not post information online that could bring the Setting in to disrepute.
- Be aware of the sanctions that may be applied for breaches of policy related to professional conduct.
- Any communications outside the agreed policies and procedures (above) may lead to disciplinary and /or criminal investigations.

Wider personal use of digital communications:

Everyone should be able to enjoy the benefits of digital technologies. Staff should separate their work relationships “friends”, from their online social life and take the following into account when using these digital communications:

- Careful consideration should be given as to who should be included as “friends” on social networking profiles and which information / photos are available to those friends
- Privacy settings should be frequently reviewed.
- Creating different ‘groups of friends’ should be considered to control what and how much information ‘friends’ can see.
- The amount of personal information visible to those on “friends” lists should be carefully managed and users should be aware that “friends” may still reveal or share this information.
- “Digital footprint” – information, including images, posted on the web may remain there for ever. Many people subsequently regret posting information that has become embarrassing or harmful to them

Personal Devices
The settings mobile phone policy is in place regarding the use of devices belonging to individuals e.g. mobile phones and cameras.

- Personal mobile phones must not be used while in the work place or to take photographs/ video images anywhere within the Settings grounds.
- Personal mobile phones are to be kept in the office at all times and not accessed until the end of the shift
- Management may permit staff to use their mobile phones as a way of emergency contact (Walking Bus or Emergency Situations)
- Management are promoted to have the work club phone on them at all times for parent/ carer communication, or emergencies

Use of digital images and video
All staff, children and young people, mothers, fathers and carers need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

As a Setting Play in Ltd will raise awareness about these risks and will implement our policies (i.e. Photograph Policy) to reduce the likelihood of the potential for harm. We also have specific policies regarding the safe use of mobile phones and cameras in the Setting.

This policy was adopted by: Play in Ltd	Date: Sept 2022
To be reviewed: Sept 2023	Signed:

Written in accordance with the Statutory Framework for the Early Years Foundation Stage (2021): Safeguarding and Welfare Requirements: Child Protection [3.4 – 3.8].