Stepping Stones Pre-School
Internet Policy

The internet is part of everyday life. Knowledge and experience of information and communication technology (ICT) should be considered as essential. Developmentally appropriate access to computers and the internet in the early years contributes significantly to children's development. Children learn best when they have managed access to computers and control of their learning experiences: however such use carries an element of risk. Early years practitioners and parents should make children aware of the risks associate with online technologies. this empowers them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

The Internet Policy aims to outline safe and effective practice in the use of the internet. It provides advice on acceptable use and effective measures to enable children and adults to use ICT resources in a safer online environment and applied to all individuals who have access to or are users of work related ICT systems. This included children and young people, parents and carers, early years practitioners and their managers, volunteers, students, committee members and other users.

The Internet Policy applies to internet access through any medium, for example computers, mobile phones and gaming devises.

The Designated Safeguarding Lead Val Cuff or Deputy Safeguarding Lead Donna Peters are responsible for online safety, and manage the implementation of the Internet Policy, they will ensure:

- day to day responsibility for online safety issues and as such will have a leading role in implementing, monitoring and reviewing the Internet Policy.

- ICT users must be made aware of the procedures that must be followed if a potentially unsafe or inappropriate online incident occurs.
- The recording, monitoring and filing of reports in the event of potentially unsafe or inappropriate online incidents will be recorded in the incident log which will be used to inform future online safe practice.
- All necessary actions will be taken to minimise the risk of any identified unsafe or inappropriate online incidents reoccurring.
- Regular meetings take place with the chairperson to discuss current issues, review incident reports and filtering/change control logs.
- training will be accessed to keep up to date with changing technological safety issues.
- Further details on the responsibilities of the Designated Safeguarding Leads are to be found in the Acceptable Use Policy.

Maintaining password security is an essential requirement for practitioners and their managers particularly where they have access to personal information. A list of authorised ICT users should be maintained and access to sensitive and personal data should be restricted.

Practitioners and their managers will be responsible for keeping their passwords secure and should ensure they are regularly updated. All ICT users should have strong passwords. Passwords should not be shared.

Computers and laptops should be set to 'time-out' the current user session if they become idle for an identified period. All ICT users must 'log-out' of their accounts if they need to leave a computer unattended.

If ICT users become aware that password security has been compromised or has been shared, either intentionally or unintentionally, the concern must be reported to the Designated Safeguarding Lead.

Internet access for all ICT users should be managed and moderated in order to protect them from deliberate or unintentional misuse. Every reasonable precaution should be taken to ensure the safe use of the internet. It has to be

acknowledge however, that it will be impossible to safeguard against every eventuality.

The following control measures will be put in place where appropriate to manage internet access and minimise risk:

- secure broadband or wireless access.
- a secure, filtered, managed internet service provider and/or learning platform.
- secure email accounts.
- regular monitored and updated virus protection.
- a secure password system.
- an agreed list of assigned authorised users with controlled access.
- clear Acceptable Use Policies and Agreements.
- effective audit, monitoring and review procedures.

Online activity will be monitored to ensure access is given to appropriate materials only.

Computers and gaming devices should be sited in areas of high visibility to enable children and adults to be closely supervised and their online use to be appropriately monitored.

If a child accidentally accesses inappropriate material, it must be reported to an adult immediately. Appropriate action should be taken to hide or minimise the window. The computer should not be switched off, nor the page closed, in order to allow investigations to take place. All such incidents must be reported to the Designated Safeguarding Lead; who must ensure a report of incidents is made and that any further actions deemed necessary are taken.

All practitioners and their managers should be made aware of the risks of connecting personal mobile devices to work-related ICT systems. Such use will be subject to explicit authorisation by the Designated Safeguarding Lead and will be stringently monitored.

Should it be necessary, the download of files or programmes to any work related system should be effectively managed and monitored.

All users are responsible for reporting any concerns encountered using online technologies to the Designated Safeguarding Lead.

All official online communications should occur where possible through secure filtered email accounts. Settings should be aware that free, web-based email services are not considered secure for personal data and their use could put the setting at risk.

All email correspondence should be subject to scrutiny and monitoring. All ICT users are expected to write online communications in a polite, respectful and non-abusive manner. The appropriate use of emoticons should be encouraged. A filtered internet server is used to monitor and prevent offensive material or spam. If on rare occasions, security systems are not able to identify and remove such materials, the incident should be reported to the Designated Safeguarding Lead.

Communication between adults and between children and adults, by whatever method, should take place within clear and explicit boundaries. This included the wider use of technology such as mobile phones, text messaging, social networks, e mails, digital cameras, videos, web-cams, websites and blogs.

When using digital communications, staff and volunteers should:

- only make contact with children for professional reasons.
- and in accordance with the policies and professional guidance of the group.
- not share any personal information with a child e.g. should not give their personal contact details to children including e-mail, home or mobile telephone numbers.
- not request, or respond to, any personal information from the child other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.

- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- ensure that all communications are transparent and open to scrutiny.
- be careful in their communications with children so as to avoid any possible misinterpretation.
- ensure that if they have a personal social networking profile, details are not shared with children in their care (making every effort to keep personal and professional online lives separate).
- not post information online that could bring the group into disrepute.
- be aware of the sanctions that may be applied for breaches of policy related to professional conduct.
- only use (wherever possible) official equipment or systems to communicate with young persons.

All ICT users are advised not to open emails where they do not know the sender or where the format looks suspicious.

Children should be enabled to use online technologies as relevant to their age and development. Access to online communications should always be monitored by a supervising adult.

Emerging technologies should be valued for the learning and development opportunities they provide for children; including a move towards personalised learning and one to one device ownership. Many existing technologies such as portable media players, gaming devices, and mobile phones will already be familiar to many children and these devices should be considered subject to the same risks as any other form of technology. Effective control measures should therefore be put in place to minimise such risk whilst maximising the opportunities for children to access such resources.

Access to a range of age appropriate websites should be enabled, but children should be encouraged to be cautious about any information given to them by other users on such sites, and must recognise that not everyone is who they say they are.

Access to social networking sites should be carefully managed within the early years setting, and children will only be permitted to use moderated child-

focused sites under supervision. Practitioners and their managers are not permitted to use work-related technologies for personal access to social networking sites.

All ICT users should be encouraged to think carefully about the way information can be added and removed from websites by themselves and others. Moderated sites can afford maximum protection.

Children and parents should know that the use of social networking sites in the home or social environment is an exciting communication tool and networking tool. It must also be emphasised however that their use can pose potential risks. Children and parents should therefore be made aware of those risks, and the control measures that can be implemented to minimise them.

Practitioners and their managers are also likely to use social networking sites in their recreational time on their own personal computers. This is not to be discouraged, however they must agree to a 'professional conduct agreement'. The use of such sites should not compromise professional integrity or bring the setting into disrepute. The adding of children and young people as 'friends' to social networking sites should be avoided.

Social networking sites and mobile technologies can be used for negative and anti-social purposes. Cyber bullying, for example, is unacceptable as is any other form of bullying, and effective sanctions must be in place to deal with such concerns. Ay known or suspected incidents must be reported immediately to the Designated Safeguarding Lead.

Emerging technologies can offer potential learning and development opportunities. Their use should be risk assessed before use by children and young people. Where necessary, further training and guidance should be provided to ensure appropriate and safe use of any new technologies.

THIS POLICY WAS ADOPTED AT A MEETING OF

THE PRESCHOOL HELD ON (DATE) .....

SIGNED ON BEHALF OF THE PRESCHOOL.....