Acceptable Internet Use Policy

Introduction

The internet should be considered part of everyday life with children and young people seen to be at the forefront of this on-line generation. Knowledge and experience of information and communication technology (ICT) should be considered an essential life skill. Developmentally appropriate access to computers and the internet in the early years will significantly contribute to children and young people's enjoyment of learning and development. This policy forms part of our Data Protection policies and procedures to ensure compliance with the GDPR (General Data Protection Regulations) and the Data Protection Act 2018.

Children and young people will learn most effectively where they are given managed access to computers and control of their own learning experiences, however such use carries an element of risk. Early Years practitioners and managers, in partnership with parents and carers, should consider it their duty to make children and young people aware of the potential risks associated with online technologies. This will empower then with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.

Policy statement

This policy will outline safe and effective practice in the use of the internet. It will provide advice on acceptable se and effective control measures to enable children, young people and adults to use ICT resources in a safer online environment.

The policy applies to all individuals who are to have access to or be users of work related ICT systems. This will include children and young people, parents and carers, early years managers and practitioners, volunteers, students, committee members, visitors and contractors. This list is not to be considered exhaustive.

This policy will apply to internet access through any medium, for example computers, mobile phones, tablets and gaming machines. Before the use of any new technologies they will be examined to determine potential learning and development opportunities.

Their use will be risk assessed before considering whether they are appropriate for use by children and young people.

Responsibilities

The Designated Person for Safeguarding (DPS) is to be responsible for online safety and will manage the implementation of this policy. In our setting the DPS are Emma Fowles, Clare Purdy and Linda Smith.

The Designated Person for Safeguarding will ensure:

- Day to day responsibility for online safety issues and will have a leading role in implementing, monitoring and reviewing this Policy.
- All ICT users are made aware of the procedures that must be followed should a potentially unsafe or inappropriate online incident take place.
- Recording, reporting, monitoring and filing of reports should a potentially unsafe or inappropriate online incident occur. This must include the creation of an incident log to be used to inform future online safety practice.
- All necessary actions are taken to minimise the risk of any identified unsafe or inappropriate online incidents reoccurring.
- Regular meetings take place with the registered person and/or managers to discuss current issues and review incident reports.
- Effective training and online safety advice is delivered and available to all early years managers and practitioners, including advisory support to children, young people, parents and carers as necessary.
- Liaison, where appropriate, with other agencies in respect of current online safety practices and the reporting and management of significant incidents.

Managing online access

Password security

- Maintaining password security is an essential requirement for early years managers and practitioners particularly where they are to have access to sensitive information. A list of all authorised ICT users and their level of

access is to be maintained and access to sensitive and personal data is to be restricted.

- Early years managers and practitioners are responsible for keeping their passwords secure and must ensure they are updated once every 60 days. All users must have strong passwords, for example a combination of numbers, symbols and lower and upper case letters.
- Sharing passwords is not considered to be secure practice. Where children and young people are to be enabled to create their own password a copy of such will be kept on file for reference.
- All computers and laptops should be set to 'timeout' the current user session should they become idle for an identified period.
- All ICT users must 'log out' of their accounts should they need to leave a computer unattended.
- If ICT users become aware that password security has been compromised or shared, either intentionally or unintentionally, the concern must be reported to the Designated Person for Safeguarding.

Internet access

- The internet access for all users will be managed and moderated in order to protect them from deliberate or unintentional misuse. Every reasonable precaution will be taken to ensure the safe use of the internet. However, it must be recognised that it is impossible to safeguard against every eventuality.
- The following control measures will be implemented which will 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.
    - Regularly monitored and updated anti-virus protection.
    - A secure password system
    - An agreed list of assigned authorised users with controlled access
    - Effective audit, monitoring and review procedures.

- Online activity is monitored to ensure access is given to appropriate materials only. Computers, laptops, tablets and gaming machines are sited in areas of high visibility to ensure children, young people and adults are closely supervised and their online use appropriately monitored.
- Should children, young people or adults discover potentially unsafe or inappropriate material, they must hide the content from view. For example, the window will minimised and/or the monitor (not Computer) will be turned off. All such incidents must be reported to the DPS who must ensure a report of the incident is made and take any further actions necessary.
- All managers and practitioners will be made aware of the risks of compromising security, for example from connecting personal mobile devices to work related ICT systems. Such use is avoided but should it, on occasion, be unavoidable it will be subject to explicit authorisation of the Designated Person for Safeguarding. Such use will be stringently monitored.
- Should it be necessary to download unknown files or programmes from the internet to any work related system it will only be actioned by authorised ICT users with permission from the Designated Person for Safeguarding (DPS). Such use will be effectively managed and monitored.
- All users are responsible for reporting any concerns encountered using online technologies to the DPS.

Online communications

- All official communications must occur through secure filtered email accounts.
- All email correspondence will be subject to scrutiny and monitoring.
- All ICT users are expected to write online communications in a professional, polite, respectful and non-abusive manner. The use of emoticons is not permitted.
- A filtered internet server is used to monitor and prevent offensive material or spam. Should, on occasions, security systems not be able to identify and remove such materials the incident will be reported to the Designated Person for Safeguarding immediately.

- Communications between children and adults by whatever method should take place within clear and explicit professional boundaries. Early years managers and practitioners will not share any personal information with any child or young person associated with the setting. They will not request or respond to any personal information from the child or young person other than which might be considered appropriate as part of their professional role. Advice should be sought from the DPS before engaging in any such communication.
- Early years managers and practitioners must ensure that all communications are transparent and open to scrutiny
- All ICT users should refrain from opening emails where they do not know the sender or where the content or format looks suspicious.
- Online communication is not considered private or confidential for safeguarding and security purposes. All users must seek advice from the DPS and the local Safeguarding Children Board as to how information should be relayed.
- Children and young people will be enabled to use online equipment and resources when it is considered, in consultation with parents and carers, that they have the developmental knowledge and understanding to recognise some of the benefits and risks of such communication. Access to online communication will always be supervised by an adult.
- When children and young people access online communications and communities a nickname must be adopted to protect their identity and ensure anonymity.

Managing multimedia technologies

- Many devices are equipped with internet access, GPS, cameras and video and audio recording functions. A risk assessment is completed to minimise risk of using technologies whilst maximising the opportunities for children and young people to access such resources.
- Access to a range of age appropriate websites are available. Children and young people are advised, in an age appropriate manner, that they should be careful whilst online and that not everyone is who they say they are.

- All ICT users and the DPS must only use moderated sites to afford maximum protection. Non-moderated websites allow for content to be added and removed by others.
- Children and young children will not be permitted to post images on any website or profile.

Social networking sites

- Access to social networking sites is not permitted by children and young people in the setting.
- Early years managers and practitioners are not permitted to use work related technologies for personal access to networking sites.
- The use of these sites in adults recreational time cannot be restricted however early years managers and practitioners must adhere to our professional conduct agreement. Content which may compromise professional integrity or will bring the setting into disrepute is not permissible and may result in disciplinary action.
- It is not permissible for early years managers or practitioners to engage in personal online communications with children, young people, parents or carers. This includes the use of social media networking platforms such as Facebook and Twitter.
- Any known misuse, negative and/or anti-social practices must be reported immediately to the DPS.