Acceptable Internet use Policy

When using social media and the Internet, the nursery will apply the same rules that would apply to the actions of employees in general; therefore, this draws no distinction between the conduct online and conduct offline. The nursery will take a view about staff actions in respect of social media and the Internet, either inside or outside of work that affect employee's work performance, the performance of others or the interests of the nursery/brand.

This policy will outline safe and effective practice in the use of the internet. It will provide advice on acceptable use and effective control measures to enable children and staff 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 including digital platform and social networking sites.

This policy will apply to internet access through any medium, for example computers, mobile phones, tablets and interactive touchscreens etc. 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.

The Management Team will ensure:

- Day to day responsibility for online safety issues and will have a leading role in implementing and monitoring the policy.
- All ICT users are made aware of the procedures that must be followed should a potentially unsafe or inappropriate online incident take place. All staff using ICT equipment within the setting should have completed relevant training.
- Recording, reporting, monitoring and filing of reports should a potentially unsafe or inappropriate online incident occur. Any incidents of misuse must be recorded on an incident reporting form and necessary action taken.
- All necessary actions are taken to minimise the risk of any identified unsafe or inappropriate online incidents reoccurring.
- 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. *Please refer to E-Safety for Children Policy.*
- Practitioners do not have access to office computers.
- Liaison, where appropriate, with other agencies in respect of current online safety practices and the reporting and management of significant incidents. (Please see bottom of page for agencies which support safer internet use)

Acceptable Internet use Policy

Managing online access

Password security

- Maintaining password security is an essential requirement for all staff 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. NO PERSONAL DATA IS KEPT ON IPADS
- Everyone is responsible for keeping their passwords secure. 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. Children are not required to create passwords for any use of internet access.
- All ICT users must 'log out' of their accounts should they need to leave an iPad /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 Safeguarding lead, and passwords must be changed immediately.
- ICT equipment belonging to the setting should remain on site at all times and portable items are to be locked away in the office when not in use where possible.

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- Children do not have access to email accounts. Staff are not required to access personal email accounts without the permission of the nursery manager.
    - Regularly monitored and updated anti-virus protection, McAfee
    - A secure password system

    - An agreed list of assigned authorised users (All members of staff) with controlled access. (The Director, manager and deputy manager will control this)
    - Effective audit, monitoring and review procedures.
- Online activity is monitored to ensure access is given to appropriate materials only. All devices 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 be minimised and/or the monitor (not Computer) will be turned off. All such incidents must be reported immediately to ensure a report of the incident is made and take any further actions necessary, informing the DSL if it is in relation to Safeguarding.
- 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 authorisation of the Designated Safeguarding lead. Such use will be strictly 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 by the manager / director with permission. Such use will be effectively managed and monitored.
- All users are responsible for reporting any safeguarding concerns encountered using online technologies to the DSL.

Online communications

- All official communications must occur through secure filtered email accounts.
- All ICT users are expected to write online communications in a professional, polite, respectful and non-abusive manner.
- All users must ensure that all communications are transparent and professional.
- All ICT users should refrain from opening emails where they do not know the sender or where the content or format looks suspicious.
- The settings email system and digital platforms must be secure password protected sites, if staff feel this is not considered private or confidential for safeguarding and security purposes it must be reported to the setting Designated Safeguarding lead.

- Websites such as YouTube, Google and other suitable search engines can be used within the setting to enhance children's learning with the use of videos, real life photos, however staff must check all content before use to ensure it is appropriate. Where internet sites are accessed, manager and staff must record which sites are agreed suitable for use. Any new websites must reviewed regularly.
- Wherever possible equipment and search engines being used by children will have parental controls
- Staff must not use ICT equipment just as a transition tool (for example sitting the children down to watch television) and it must only be used to enhance children's learning and development.

Digital Platforms

Tapestry may be stored using a digital platform, which enables practitioners and managers to capture, assess and track learning and development for the children in the nursery. It uses secure servers to store personal information, including photos and videos and can be accessed by parents also.

Staff must be aware of the following when using Tapestry:

- Tapestry contain confidential information about the children and their families, including photos and videos of the children, and some personal information
- Staff should only login to Tapestry using their own password and pin code, unless authorised
- Staff should not share their personal login information with others
- Staff are strictly prohibited from using Tapestry on any personal devices
- The safe and appropriate use of Tapestry will be regularly monitored
- Media or data is not to be transferred to any external storage device or shared via the Internet without the consent of the Nursery Manager.

Managing multimedia technologies

- Many devices are equipped with internet access, GPS, cameras and video and audio recording functions. Using technologies whilst maximising the opportunities for children and young people to access such resources.
- Access to a range of age-appropriate websites is 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. Children are not allowed access without an adult present and overseeing the process.

- Children and young children will not be permitted to post images on any website or profile.
- Internet usage by children will be used supervised for research and extension of learning purposes only

Social networking sites

- Access to social networking sites is not permitted by children / young people / staff in the setting.
- When requested, staff are permitted to post on the setting's social media account about activities which they have carried out. List of permissions must be followed at all times.
- All staff are not permitted to use work related technologies for personal access to personal networking sites.
- The use of these sites in adult's break times cannot be restricted via adults' own devices 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 advised for staff to engage in personal online communications through their personal accounts with children, young people, parents or carers. This includes the use of social media networking platforms such as Facebook, Instagram, Snapchat and Twitter.
- Any known misuse, negative and/or anti-social practices must be reported immediately to the DSL.
- Nursery Facebook and Instagram and brand specific social network sites for marketing and shared professional platforms are permitted for their intended use only

Further guidance

- NSPCC and CEOP *Keeping Children Safe Online* training: www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/

  https://www.nspcc.org.uk/keeping-children-safe/online-safety/internet-connected-devices/

- Kelsi.org.uk
  https://www.kelsi.org.uk/child-protection-and-safeguarding/e-safety/e-safety-classroom-materials

- Pacey –
  https://www.pacey.org.uk/working-in-childcare/spotlight-on/online-safety/

Acceptable Internet use Policy

- GOV.UK
  https://help-for-early-years-providers.education.gov.uk/safeguarding-and-welfare/internet-safety

  https://www.gov.uk/government/publications/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-considerations/safeguarding-children-and-protecting-professionals-in-early-years-settings-online-safety-guidance-for-practitioners

Linked Policies

Safeguarding & Child Protection Policy
E-Safety Policy
Whistleblowing Policy
GDPR Policy
Staff Code of Conduct

This policy was adopted on	Signed on behalf of the nursery	Date for review
16/1/2023	*m khaira*	*16/01/2024*