Kiddy Academy Digital Technology & Social Networking Policy

This policy links to:

- **EYFS** statutory requirements – the provider must take necessary steps to safeguard and promote the welfare of the children.

- **EYFS** A unique child: 1.3 Stay safe

We believe our staff should be completely attentive during their hours of working to ensure all children in the nursery receive good quality care and education. One of the reasons why mobile phones are not to be used during working hours.

Therefore personal mobile phones, ipad (or equivalent) or cameras are not permitted for use within the Nursery by either Staff or parents/carers. (In designated staff room only)

We also feel that restrictions need to be placed on staff when they access social networking sites. Kiddy Academy Day Nurseries has a high reputation to upkeep and comments made on sites such as 'Facebook' could have an impact on how parents using the nursery and view the staff.

- Mobile phones must not be used unless on a designated break In a designated area and under no circumstances in a nursery room as this will result in instant dismissal
- Mobile phones should be stored safely in the box in the office throughout the working day.
- Mobile phones MUST NOT be used to record any child during their time at the nursery or when on an outing. Doing so will result in disciplinary action.
- Parents must not use their mobile phones or recording devices on the nursery premises where children are present, unless permission is sought during social events such as graduation parties or visits from Santa etc.
- Staff must not post anything onto social networking sites such as 'Facebook' that could be construed to have any impact on the nursery's reputation
- Staff must not post anything onto social networking sites that would offend any other member of staff or parent using the nursery
- If staff choose to allow parents to view their page on social networking sites then this relationship must remain professional at all times, and must not contain any reference to Kiddy Academy Day Nursery or the children in our care
- We will also monitor what the children are exposed to when they access the internet and ensure they only have access to age appropriate sites and images. We will ensure they do not share any personal information or images with any other party.

Internet, WIFI, Email and Password Use

In today's modern society, the use of the internet features in almost every workplace including childcare f
schools. Children are increasingly making use of this technology and as a result internet usage is on the r
settings now have computers and tablets that are connected to their WIFI and internet to aid children's te
development.

As practitioners it is our duty to ensure that children are provided with managed access to the internet, bu
ensure that children are kept safe from potential inline risks. As practitioners we want to enhance a ch
through technology and of course keep them safe, without limiting their learning opportunities and experie

This policy will also illustrate how we monitor staff, volunteers, students, managers, practitioners and parental usage of the internet when they are using our devices.

As a setting, our main priority is to keep individuals safe when accessing any of our technological devices, whilst not limiting learning opportunities or enjoyment. New devices entering the setting will be risk assessed accordingly as will fair use in order to identify 'over use' or abuse of usage.' Adults and children are not permitted to use our internet or devices for personal use.

The Designated Safeguarding lead is to be responsible for the online safety and will manage the implementation of this policy. The Designated Safe

The Designated Safeguarding lead roles involves implementing, monitoring and reviewing this policy. They also ensure that all individuals using our devices and making use of our ICT technology are fully aware of their roles and responsibilities. The DSL will make users aware that procedures must be followed to ensure appropriate and fair use.

The DSL is responsible for ensuring that all inappropriate use is recorded appropriately, and the correct form filling procedures are adhered to. The DSL will record any inappropriate use, which is then used to inform future online safety practice. The DSL also ensures that regular meetings take place with the registered person and/or managers in order to discuss current issues, review current practice and also to consider any incident reports and how they should be acted upon.

The DSL is also responsible for ensuring that any training and online safety advice is delivered and is available to all early year's managers and practitioners within the setting, including advisory support to children, young people, parents, and carers. Where necessary the DSL will liaise with other agencies in respect of current online safety practices.

Password security – Online access

Protecting data is imperative and is required by the GDPR Law, therefore maintaining password security is an essential requirement for our setting. All staff are required to have passwords to access tapestry and the settings devices. In our setting, we have a list of users that are authorized to access data on tapestry, and this list provides details of the level of access each person has. We advise all users to use strong passwords that consist of numbers, capitals, lower case and characters to ensure that no one else can guess the password. We do not endorse in any shape or form the use

of sharing passwords. This is considered as bad practice and could result in a breach of data. Passwords can be regenerated on our system in the event of a lost password. Once the person has left the setting we follow procedures to ensure they can no longer access the account. Our computers, laptops, and tablets are all set on 'Timeout' devices, which means if they are left unattended and idle for some time, other users cannot begin accessing data without consent.

All device users must 'log out' of their accounts should they leave a computer unattended. If they do not and data is breached this could result in disciplinary measures being taken, and in some cases prosecution.

In the event of password security breach, users are asked to report immediately to the DSL. If device 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.

Access to the setting's internet

To ensure that the internet is used for the appropriate purpose, we will manage and moderate usage to protect users from unintentional or deliberate misuse. As a setting, we will do all we can to protect the users, but in the event of inappropriate usage, the DSL will investigate the matter and update current policies and procedures to avoid such breaches again.

The following control measures have been implemented within our setting to ensure that internet breaches are avoided. In our setting we have implemented:

The settings broadband can only be accessed by those that work at our setting and devices are set to the settings broadband and is password protected. The access code that we use for broadband is given to only those that require it and is changed every 6-8 weeks.

Our emails are only accessed by members of the senior management team. Those individuals that have controlled access are aware of their responsibilities to maintain confidentiality.

Online activity is monitored by members of the management and staff team. This ensures that only appropriate materials via the internet can be assessed by individuals. All devices including computers, laptops and tablets are password protected and monitored. They are sited in areas of high visibility to ensure children, young people and adults are closely supervised and their online use appropriately monitored. In the unlikely event that inappropriate material is accessed. The

incident will then be reported to the DSL who will ensure that an appropriate report is written, and the incident investigated accordingly.

In the event a virus contaminates our devices, we will call our provider to support us in our endeavor to keep our devices free of threat.

If practitioner feels that it be necessary to download unknown files or programmes from the internet to any work-related system, then this will have to be authorized by the DSL to test the authenticity of any given site and to make sure practitioners do not download inappropriate material. Individuals are responsible for reporting any concerns that they may have whilst they are using our devices online; they are instructed to report this immediately to the DSL.

Communication - online

As stated earlier, our emails are password protected. Staff are informed that all email correspondence is subject to scrutiny and monitoring. This is to protect the user and those receiving the email. Those using the setting email address must write to individuals in a professional, polite and respectful manner. It is not permitted for staff to send abusive emails or unauthorized emails. We also do not use emoticons in any of correspondence, and professionalism must be upheld at all time.

Staff are not permitted to use 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.

Individuals within the setting are not permitted to share any personal information with any child/young person associated with the setting. This includes sharing information via Facebook, Instagram or any other informal social media means. 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 DSL before engaging in any such communication.

All communications sent from our setting will be transparent and open to scrutiny. It is the policy of this setting, and in the interest of device security, that users do not open any emails or documents that come from an unknown source. We are aware that online communication can be considered unsafe, not confidential and open to risk. Our settings policy is to seek the relevant support and advice from the DSL and from the LSCB.

Practitioners in our setting will monitor the online activity of all children and access to online communication will always be supervised by an adult. It is the policy of our setting when allowing children to access various online social games or apps, to adopt an alias to protect the identity of the children. This is to ensure that the anonymity of the child engaging in such online communication is protected, and the child's identity and the location are not compromised.

We carry out thorough risk assessments on all our devices including recording equipment, cameras, and video devices. Children and practitioners have access to a range of appropriate devices within the setting, and all are trained accordingly to use them appropriately and to treat them with respect.

It is our policy not to allow children to upload any images of themselves or that of others onto the internet. Children are permitted to take photographs, and to print them, but are prevented from uploaded and sharing them online.

Social Media

It is the policy of our setting to prohibit the unauthorized use of social media networking sites such as Facebook or Instagram by the children. We do not create any profile accounts for any of the children within our care. Practitioners are also asked not to use such sites on their own devices whilst at work, and they are forbidden to take any photographs of the setting or the children and share them on their private accounts. Furthermore, practitioners are not allowed to use work devices to access their own account; this is strictly forbidden. We acknowledge that practitioners will have their own social media profiles, but we do insist that they adhere to our code of conduct agreement which staff is obliged to sign. Any content that may compromise the professional integrity of our settings, or bring our setting into dispute or put any child at risk could result in disciplinary action being taken against the staff member, in extremely serious cases, staff may be prosecuted. Staff are also aware that they are not to engage in personal online communications with children, young people, or parents and carers either through email or via social networking sites unless the relationship remains professional. This is to ensure the protection of staff and the protection of children and parents/carers. In the event of any known misuse or negative and anti-social practices via such social networking mediums, staff may face disciplinary action.

Childcare at its Best

Review date: 16.01.18	Date of next review: 16.01.19