## Safe guarding Children

## 2.14 Internet, email and password policy

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

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

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 Safeguard Lead in our setting is

| |
|---|
| Rachel Cottrell |

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 issue in

the settings incident Log book, 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, which are changed every term for security reasons. In our setting, we have a list of users that are authorized, and this list provides data on who is responsible for which device as well as the level of access each person has on each device. 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. Where possible passwords are encrypted. 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 gone the strict security procedures to ensure the account that they are trying to access is in indeed their 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.

## Communication - online

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 must also copy in their manager, or the manager of the setting, the owner, must be copied in. This ensures quality control and allows for professional email monitoring of colleagues.

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.

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.

Our managed systems allow only authorized websites to feature on any device, and any unauthorized websites are barred from ever been downloaded. It is our policy not to allow children to upload any images of themselves or that of others onto any of our devices.

## 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 professional 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 is 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. 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.

This policy was adopted at a meeting of _____

Held on _____ (date)

Date to be reviewed _____ (date)

Signed on behalf of the management committee _____

Name of signatory _____

Role of signatory (e.g. chair/committee) _____