Rainbow Early Years

E-Safety policy

(Including:
Acceptable use (AUP)
ICT
Online Safety)

Statement of intent

It is our intent that all users at Rainbow Early Years (REY) can benefit and learn from the technologies offered in a safe and effective manner.

Aim

We aim to ensure that both adults and children are able to access and safely use Information, Communication Technology (ICT) at REY.

Methods

In order to achieve this aim, we operate the following policy.
Equipment

- The children attending REY will have access to tablet computers and age appropriate downloadable software. This will be kept in the play room at all times. Also some child friendly Amazon fire tablet computers are available.
- For the exclusive use of the staff at REY will supply internet enabled Tablets and these will be located in the Meeting room and Office and secured in a locked cabinet when not in use.
- Other technology equipment e.g. music players, digital cameras, interactive toys, calculators, programmable toys, etc. will be stored in a suitable place and used as part of the children's play.
- All equipment will be maintained and updated by REY as necessary. Appropriate and up to date virus protection will be installed on all computers.
- Only equipment specifically supplied for use at REY is to be use within the pre-school, adults are not permitted to bring in or use items from home in daily practice that have not been PAT checked/tested, such as laptops.
- PAT testing carried out annually for moveable electrical equipment.

Acceptable use of computers

- At REY we are aware of the value of technology in the overall learning of the children that attend and as such all children have equal opportunity to use such equipment.
- All children will be supervised at an appropriate level by an adult when using technology equipment, support and encouragement will be given at all times.
- Child friendly websites will be used and parental restrictions will apply when children are using a tablet computer.
- Staff tablet computers are password protected.
- Staff members have access to the internet whilst at work through the computer kept in the office and laptop. Adults working at REY are not to use mobile phones or other mobile devices to access the internet whilst at work.
- All staff members must be aware that viewing or using inappropriate websites using equipment supplied by REY will lead to disciplinary procedures, and could necessitate instant dismissal. Ofsted will always be informed of any such actions.
- Permission for personal use of REY's computer by a member of staff must be sought from the Manager or Chair of committee and will be restricted to outside of working hours only.

Mobile phones

- The use of mobile phones by any member of staff is limited to emergencies only and, alongside personal belongings, must be stored either in a cupboard in the Meeting room or in the Office (please refer to the staff code of conduct for more information).
- Mobile phones can only be used by an adult when they are in either the Meeting room or Office and only use at breaktime only if there are no children present.
- It is not expected that any child attending REY will have a mobile phone of their own. If they should bring one in then a member of staff must ensure that it is turned off and stored safely till the child goes home. (This also applies to SMART watches).
- The group will provide blank or dummy phones and other such equipment for the children to use in their play.
- At **no** time will mobile phones be used to take photographs at REY.
- All visitors are expected to leave mobile phones or any other portable device secure in their bag and will be kept safe in the office whilst visiting.
- REY has a mobile phone which can be used on trips out of the setting for contact or when Forest School activities take place.

REY website

- REY has its own website that is used for information purposes only.
- This is maintained and updated by a member of staff.
- It is paramount that if photographs of the children attending REY are to be used on the website they must not be individually identifiable and that specific parental permission is gained.
- No personal information such as names, addresses or dates of birth will be disclosed through the website, confidentiality will be maintained at all times.
- Links to other websites may be displayed on the website, but REY cannot be responsible for the content of external sites.

Email

- All members of staff are welcome to use REY's office 365 email address for work purposes only.
- Members of staff may request, through the Manager, to have their own personal email address at REY. This may then be used to receive mails of a sensitive nature which could present a safeguarding issue should other members of staff read them.
- Staff are aware that they are not to use abusive, threatening or intimidating language within any email that they write, if they receive any such message they must immediately pass it on to the Manager/Chair for a response.
- Parents are given the email address of REY when their child first starts with us and are welcome to use it as a method of communication with us.
- If anyone misuses our email system they will be blocked from further use.
- Newsletters and letters will be distributed via email to parents who have shared their email address.

Social networking

- When off duty, members of staff should show caution when using such sites (please refer to the staff code of conduct for more information).
- REY will have their own closed Facebook group page and invite parents and carers to become 'friends'.
- Facebook offers REY an alternative method of communicating with adults associated with the group and 'posts' are only to be made from REY about specific events associated with the group.
- Should a 'friend' write abusive, intimidating or unfriendly messages that can be viewed through the REY page they will be immediately blocked.

- The Manager monitors the Facebook page to ensure the quality of posts.
- When parents/carers or staff leave the setting they will be taken off the closed Facebook group buy the Administrator or Manager.

Interactive Learning Diary (ILD)

- Every ILD staff and parent user has their own secure and unique username and password.
- ILD have a comprehensive security and privacy policy see below; for further information please visit http://www.interactivelearningdiary.co.uk/

At the Interactive Learning Diary (ILD) we have an advanced set of security measures to protect your information. We take your data security very seriously and have developed a comprehensive set of practices, technologies and policies to help ensure your data is secure.

- Our data centres are based in two different locations in the U.K in some of the most secure facilities available today and are protected from physical and logical attacks as well as from natural disasters such as earthquakes, fires, floods, etc.
- We use 128-bit SSL encryption for all data transferred between your mobile device, computer and our servers. The whole system is protected by a secure SSL certificate which means that any data sent is highly encrypted so no one can intercept the information.
- The data encryption software which we use is fully PCI and HIPAA compliant and a market leader in this field. This software is also used by various U.S. government agencies, international banks and companies.
- Every setting has its own dedicated database, therefore eliminating any possibility of cross contamination. This database will only ever store your data which will always belong to you.
- Every ILD staff and parent user has their own secure and unique username and password.
- The ILD system and all our key hardware have automatic redundant backups so no data will be ever be lost. Additionally, all of your data is backed up to a secure location in the U.K, still in its encrypted form, so a full backup recovery can be performed if required.
- When using our mobile apps on your phone or tablet, upon successful transfer of data to the ILD web application, all child data is automatically deleted from the device. This security feature ensures if the device is ever lost or stolen, there is no access to confidential data.
- All personnel working with or who are part of the ILD team are fully DBS & PVG checked at enhanced levels. This forms part of our rigorous recruitment procedures.

This individual policy forms part of a larger policy document and should be read alongside our other individual policies.
Date adopted for Rainbow Early Years: January 2011

Date of last review: 4th August 2020 by the Manager.
Date of next review: _____