

# **I.C.T (INFORMATION, COMMUNICATION AND TECHNOLOGY) POLICY**

## **Aim**

At Jellytots we limit the use of ICT to research, encouraging discussion, and whole-group learning activities as we acknowledge the harm of excessive screen time.

Refer to pages 11 and 12 of our Safeguarding and Child Protection Policy

## **Jellytots principles are as follows:**

To continue to develop good practice in the use of ICT we will;

- Make sure that ICT resources are appropriate for both the Early Years curriculum and children's technical ability
- Keep up to date with ICT initiatives and software.

To reflect upon and promote equality and inclusive practice we will;

- Recognise, value and use children's experience of ICT outside the early years setting as an important learning resource.
- Support and value cultural identities and diversity by appropriate use of the internet.
- Be aware of the range of resources that can be particularly effective in promoting inclusive practice.
- Maximise the potential for using ICT to support continuity in children's learning.

To ensure that all children have access to and opportunities to learn about ICT we will;

- Be aware of Health and Safety guidelines relating to the use of ICT.
- Include Jellytots on adjoining school intranets.
- Ensure that internet access is only available when supervised by an adult and on the managerial laptop.

To develop and support professional ICT development for all staff we will;

- Use existing skills, knowledge and expertise to develop ways of incorporating ICT across the curriculum.
- Consider how best to provide continuous professional development on the value and use of ICT

## **Data**

- All members of staff are aware of the GDPR (General Data Protection Regulations) and data stored on any Jellytots computer will not breach the requirement of that legislation.
- A Password and/or Identification Code will protect any personal data that is stored locally on a computer. These passwords are changed regularly.
- Data and software will be maintained within secure user groups.
- No digital photographs will be shared via the internet without prior written permission from parents (**\*see statement below**) Images of children are copied onto USB Sticks as part of

the progress record of the child, these will then be printed as photographs for a child's folder. To do this, photographs will be downloaded termly by the Manager Jan John onto Bootsphotos.com who are powered by 'CEWE'. The company states:

**\* Keeping your personal information secure**

***CEWE Data Protection***

***We respect your privacy at CEWE. All data collected is used to improve our product offering. Data protection and data security for customers and users is of paramount importance at CEWE. The protection of your personal data throughout our entire business processes is therefore a particular concern to us.***

**\* Collection and Processing of Personal Data**

***When you visit our website, our web servers temporarily store access details as standard, i.e. the IP address of your access, the session\_ID to identify your connection session, as well as the date and time of your visit.***

***This data is deleted at the end of your use of the site.***

The photographs are returned by courier to the Manager who then distributes them to the staff ready to be put into your children's Learning Journey folders.

- Any photographs or moving footage of children taken whilst at Jellytots will be removed/deleted from all computers, cameras, USB storage sticks and albums held at Boots 2 weeks after the end of the term in which they leave our setting for school or another setting.
- A Facebook page is maintained by the Manager. Access is limited to staff, current parents and close family. Parental permission is obtained for photographs and moving footage of children to be posted. Access is removed when children leave the playgroup.
- Copyright of materials and intellectual property rights must be respected. Sufficient licenses have been purchased and can be demonstrated to cover actual and possible usage.
- Any computer must have virus protection installed and operational. Disks containing data from an outside source should not be used without permission.

*Policy Amended on 19<sup>th</sup> March 2025 – R Cockbill Chairperson*