



ICT and Data Protection Policy

This policy applies to all staff, including senior managers, paid staff, volunteers and sessional workers, agency staff, students or anyone else working on behalf of Mulberry Corner.

Information and Communications Technology ("ICT") involves the manipulation, interpretation and creation of learning and play through images, data and equipment electronically. At Mulberry Corner activities are designed to give children the opportunities to achieve high levels of age related developments in ICT skills using a wide range of ICT, both through computer and non-computer based experiences.

The purpose of this policy is:

- To clearly identify the rationale for using ICT in a nursery setting;
- To set out the principles of practice to ensure ICT is used safely, creatively and successfully to enrich learning, play and developmental experiences;
- To support employees to undertake their roles professionally and efficiently;
- To outline safe and effective practice in the use of the internet including effective measures to enable children and adults to use ICT resources in a safer online environment;
- To set out the rules for processing, storing and using personal data (both in paper and digital format).

Legal Framework

This policy has been drawn up on the basis of law and guidance that seeks to protect children, namely:

- Computer Misuse Act 1990;
- Data Protection Act 1998;
- Communications Act 2003;
- Malicious Communications Act 1988;
- Telecommunications Act 1984;
- Criminal Justice & Public Order Act 1994;
- Racial and Religious Hatred Act 2006;
- Protection from Harassment Act 1997;

- Protection of Children Act 1978;
- Sexual Offences Act 2003;
- Public Order Act 1986; and
- Obscene Publications Act 1959 and 1964.

This policy links to:

- The Early Years Foundation Stage (DfE 2012) Statutory Framework – setting the standards for learning, development and care for children from birth to five;
- Our Safeguarding Policy;
- Our Health and Safety Policy;
- Our Mobile Phone Policy;
- Our Image Consent form; and
- Our Staff Acceptable Use Agreement.

Use of ICT

- ICT is used throughout the nursery on a daily basis by both staff and children. ICT is of great benefit in supporting a close partnership with parents through the website, our blog, email communication and Tapestry.
- ICT is embedded throughout the EYFS and integrated into life within the nursery. ICT is extremely important as a tool for staff to communicate, record, plan, assess, email and print.
- Children are offered the opportunity to enjoy using ICT and have access to cameras, computers, sound recording devices, battery operated toys, our CD player etc. All children are taught how to treat all ICT equipment with respect and care.
- By creating opportunities to investigate, trial and experience technology, children will learn for themselves whilst being taught skills and knowledge to enable them to build upon what they already know. By carefully planning our play areas to reflect the world we live in, children are able to play, gain experience and an understanding of ICT.
- In our preschool, time is allowed for independent use of ICT, in which the children have the opportunity to explore and experiment. One to one ICT sessions are also on offer in our preschool to the children weekly.
- Children are encouraged to use ICT equipment throughout all areas of their learning.
- Children initially use any piece of ICT equipment under adult-led supervision but shall be given the opportunity to use such equipment independently as soon as is appropriate.
- Both the main nursery and our preschool has access to at least one tablet and a digital camera (“nursery equipment”) which they can use during the nursery day.
- All photographs in the nursery must be taken through the nursery equipment. Staff are not permitted to use any other digital devices to take photographs of the children. Photographs may be edited and/or used in a child’s online learning journal, our monthly newsletter, on our website or on our blog.

Roles and responsibilities

- Emma Sadler (the “ICT Leader”) has overall responsibility for ensuring the safety (including online safety) of all staff, volunteers and members of the group, though day to day responsibility for online safety may be delegated to others including deputy managers, supervisors and the Lead Practitioner for Safeguarding (“LPS”).
- The ICT Leader and the deputy managers should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff or volunteer.
- The ICT Leader shall ensure that all staff and volunteers have an up to date awareness of the nursery’s current online safety policy and practices and are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- The ICT Leader:
 - Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the online safety policies/documents;
 - Offers advice and support for all users;
 - Keeps up to date with developments in online safety;
 - Understands and knows where to obtain additional support and where to report issues;
 - Ensures provision of training and advice for staff and volunteers;
 - Communicates with parents and carers.
- The ICT Leader should be trained in online safety issues and be aware of the potential for serious child protection issues.
- Staff and volunteers are responsible for ensuring that:
 - They have an up-to-date awareness of the nursery’s current online safety policy and practices;
 - They have read, understood and signed the Staff Acceptable Use Policy (“AUP”);
 - They report any suspected misuse or problem relating to ICT to the ICT Leader or the LPS, particularly where it is believed that a child’s welfare is at risk;
 - They are aware of online safety issues, particularly those related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement the nursery’s policies with regard to these devices.
- Members of staff who are confident with ICT are encouraged to support less competent members of staff to develop their ICT skills. Staff are always welcome to ask for help, support or advice.
- Staff utilise ICT to access e-learning opportunities to enhance their skill base – e.g. Prevent training, FGM Training, Safeguarding Training etc.
- It is recognised that parents and carers also play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

Internet safety

- The internet is part of everyday life. Knowledge and experience of ICT should be considered essential. Developmentally appropriate access to computers and the internet in the early years contributes significantly to children's enjoyment of learning and development.
- Children learn most effectively where they are given managed access to computers and control their own learning experiences; however such use carries an element of risk. Early years practitioners, their managers and volunteers, alongside parents and carers, should make children aware of the potential risks associated with online technologies. This empowers them with the knowledge and skills to keep safe, without limiting their learning opportunities and experiences.
- Mulberry Corner has created a monitoring log and a reporting log in which incidents or problems are recorded by staff during ICT sessions or in relation to a potentially unsafe or inappropriate online incident taking place. These logs are used and reviewed to inform future online safety practice.
- Regular meetings shall take place with the ICT Leader, the LPS and the deputy managers to discuss current issues and review monitoring and reporting logs.

Password security

- Maintaining password security is an essential requirement for early years practitioners and their managers particularly where they have access to personal information.
- Early years practitioners and their managers will be responsible for keeping their passwords secure and should ensure they are regularly updated. All ICT users should have strong passwords. Passwords should not be shared.
- If ICT users become aware that password security has been compromised or has been shared, either intentionally or unintentionally, the concern must be reported to the ICT Leader or the LPS.

Internet access

- Internet access for all ICT users is managed and moderated in order to protect them from deliberate or unintentional misuse. Every reasonable precaution is taken to ensure the safe use of the internet. It has to be acknowledged however that it will be impossible to safeguard against every eventuality.
- The following control measures are in place to manage internet access and minimise risk:
 - Secure broadband access;
 - Child friendly filtering systems to prevent adult content being available through the internet on any electronic device used whilst at nursery;
 - Secure email accounts;
 - Regularly monitored and updated virus protection;

- Secure password system;
- Clear Acceptable Use Agreements and Policies;
- Effective audit, monitoring and review procedures.
- Online activity is monitored to ensure access is given to appropriate materials only.
- Computers are sited in areas of high visibility which enable children and adults to be closely supervised and their online use to be appropriately monitored.
- If a child accidentally accesses inappropriate material, it must be reported to the ICT Leader, LPS or a member of the management team immediately. Appropriate action should be taken to hide or minimise the window. The computer should not be switched off, not the page closed, in order to allow investigations to take place. All such incidents must be reported to the LPS, who must ensure a report of the incident is made and that any further actions deemed necessary are taken.
- All early years practitioners and their managers should be made aware of the risks of connecting personal mobile devices to work related ICT systems. Such use will be subject to explicit authorisation by the ICT Leader and will be stringently monitored.
- All users are responsible for reporting any concerns encountered using online technologies to the ICT Leader or the LPS.

Online communications

- All email communications should be made via the nursery's email account (childcare@mulberrycorner.co.uk). Only the owners, the ICT Leader, the Manager, the deputy managers and the LPS shall be permitted to communicate via these email accounts on behalf of the nursery, unless express permission has otherwise been given by the ICT Leader.
- All ICT users are expected to write online communications in a polite, respectful and non-abusive manner.
- All ICT users are advised not to open emails where they do not know the sender or where the format looks suspicious. Instead they should report the email in question to the ICT Leader.
- Children should be enabled to use online technologies as relevant to their age and development. Access to online communications should always be monitored by a supervising adult.
- All ICT users should be encouraged to think carefully about the way information can be added and removed from websites by themselves and others. Mulberry Corner uses a tailored filtering system which restricts social media sites and pornographic/adult content or material.
- Early years practitioners and their managers are also likely to use social networking sites in their recreational time on their own computers, mobile phones and/or tablets. This form of activity is not to be discouraged, however all staff must agree not to compromise their professional integrity or bring the nursery into disrepute. The adding of parents and carers as "friends" to social networking sites is not permitted unless such parents/carers were personal friends prior to their child joining the nursery.

Personal Data

- The nursery and its staff may have access to a wide range of personal information and data, held in digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:
 - Personal information about children, members of staff/volunteers and parents and carers (e.g. names, addresses, contact details, legal guardianship details, health records, disciplinary records);
 - Professional records (e.g. employment history, taxation, national insurance numbers, appraisal records and references);
 - Any other information that might be disclosed by parents or carers or by other agencies working with families.
- It is the responsibility of all staff and volunteers to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not have permission to access that data or does not need to have access to that data. Anyone who has access to personal data must know, understand and adhere to this policy.
- The nursery will hold the minimum personal information necessary to enable it to perform its function and information will be erased once the need to hold it has passed.
- Every effort will be made to ensure that information is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- Mulberry Corner Nursery & Preschool is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.
- Staff and volunteers will receive data handling awareness and data protection training and will be made aware of their responsibilities as set out in this policy through:
 - Induction training for new staff;
 - Staff meetings;
 - Day to day support and guidance from the ICT Leader.
- Personal data must be held securely on the nursery's premises and only accessed by those with permission to do so. Any personal data removed from the premises should have the appropriate level of protection to prevent loss of data.
- Mulberry Corner recognises that under Section 7 of the Data Protection Act 1998, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Any Subject Access Requests made to the nursery in writing will be dealt with promptly by the ICT Leader.
- Mulberry Corner will comply with the requirements for the safe destruction of personal data when it is no longer required. Such data must be destroyed, rather than deleted and be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, and paper based media must be shredded.