



Name:	Date:
Acceptable Use of Technology Policy	18/2/21
Written by:	Date of Review:
Emma Holmes/ Louise Lloyd-Evans	13/9/23
Policy Statement	
This policy is to ensure staff understand and use technology in a safe, legal, and correct manner. It also ensures that staff take care of any expensive I.T items, in line with our sustainability ethos.	
Aims and Purpose	
<p>We safeguard children and staff by promoting appropriate and acceptable use of all technology, taking steps to protect property and people from accidental damage and online criminal behaviour.</p> <p>All individuals who have access to, and are users of, any work-related technology systems must be clear about their roles and responsibilities including having an awareness of risk, cyber security, a clear understanding of what constitutes misuse (unacceptable behaviours) and the sanctions that may be applied. We acknowledge that the information we hold is valuable to a criminal.</p>	
Applicability	
Staff Children Families	
Definition of Terms	
Technology: Computers, walkie talkies, mobile phones, phones, laptops, tablets, internet, email, CCTV, Family app, social networking sites, smart watches, cameras, Almas fingerprint system and any other technological and recordable device. As well as the data that is stored on them.	
Overview	
Family Photographic Devices Computers, Tablets and Laptops Mobile Phones	

CCTV

Walkie Talkies

Social Networking

Almas Finger-print System

Maintenance and Care

Procedures

- All technology must not be used to access anything illegal, harmful, or inappropriate.
- All staff must immediately report any illegal, harmful, or inappropriate material.
- All staff are responsible for monitoring the behaviours of all practitioners, parents and carers, visitors, and contractors. Safeguarding is everyone's business, and this must be promoted at all times.
- To comply with the Data Protection Act 2018 and GDPR the setting is registered with the Information Commissioner's Office as a data controller to allow us to store digital images on an SD card device/computer (see certificate in office).

Family – our online parent portal.

- Family is fully compliant with the EU's General Data Protection Regulation (GDPR). On top of this, their server provider Amazon Web Services (AWS) has been approved in accordance with the EU Data Protection Directive.
- Family's data is stored in an industry standard AES-256 encrypted database.
- We ensure parents/carers can always reach the setting via Family. We encourage this to be the main method of communication in adherence to our communication policy.
- Parents' permission is gained on admission to take any photographs or videos of their child to record experiences and share their progression on the Family app (see images policy).
- The manager and the deputy manager have permission to have the app on their mobile devices in case of emergencies and for staff and children registers during a fire evacuation (please see Fire and Evacuation Policy).
- Staff must keep the use of the Family app to a minimum during working hours and use time allocated to communicate with parents wisely and within agreed protocols.
- Staff must receive special permission to access Family from home and this will be monitored by management. For example, if a staff member is having a 'work from home day' to catch up on paperwork/ do apprentice study etc.

Photographic Devices (see Images Policy)

- Any photographs or videos taken are stored appropriately, used, and deleted in accordance with our data protection and privacy policies.
- We take photos/images with nursery iPhones, which do not have sim cards.
- These iPhones are also used to take photos for social media, where we only show photos of unidentifiable children.

- We have a nursery trip phone which we also use to take photographs. This is deleted regularly and is the property of the nursery.

Computers, Tablets and Laptops

- Anti-virus software is used on devices when available.
- We will ensure the safety of all children in attendance, providing them with appropriate access to material whilst using the internet, supporting them to use technology.
- When children are ready, we talk to them about people who can be unkind and relate this to online. We do this through stories, persona dolls and discussion when we feel this time is right and link this to keeping safe and healthy when using technology.
- All computers, tablets and laptops must be stored safely and securely our locked device cupboard every evening and at weekends. They must be password protected where possible, kept in good working order and not taken off the premises unless given express permission.
- Staff must give other professionals the Young Friends management email only and ask them to put FAO [staff member] in the subject bar. Emma will copy the email into Famly, and a response will be given by the staff member and dealt with on a case-by-case basis. Staff must never give a family, professional or service associated with Young Friends their personal email. Staff must not email any information from the Young Friends computers to their personal email under any circumstances.
- No staff member will copy, remove, or otherwise alter any other user's files, without authorisation. They will not download or install anything that they do not have the right to see or use.
- Emails, calls and all communications to us are screened for phishing, unusual requests, impersonation of a professional and no information is passed on until the destination is checked out and verified.
- We use OneDrive to back up and share files. This can only be accessed by management.
- Staff are supported through induction and training to keep themselves safe online
- With regards to Prevent Duty (see policy), there has been a significant rise in the number of children radicalised online by right wing extremists/narratives. Figures show a 7% increase in the volume of terrorist content online during Covid-19 and lockdowns. Even though our children don't access any IT without an adult present and they are very young, we know it is important that we equip them with the necessary skills and knowledge to foster a positive relationship with technology.
- Staff will not show children any inappropriate online content. All online content should be agreed by Pod Leads, the Deputy or the Manager. All films, film clips, songs and images will be age appropriate and U rated.
- If we watch any online content which may provoke conversation later at home, we will share it with parents on Famly.

Mobile Phones and Smart technology – personal and nursery

- Any visitors to the setting will be asked not to use their mobile phones.

- Mobile phones and Smart Watches must be stored in their relevant lock boxes and can be used during lunch breaks only.
- The Young Friends phone must be checked regularly for messages.
- Handheld devices must be labelled and kept in the base when not in use. Staff can use the Young Friends phone with permission.
- Personal recordable devices including Smart watches are not allowed to be worn during working hours.
- Nursery iPhones do not have sim cards and are used to take photos/videos or access Family.
- Designated trip leaders take the nursery trip phone for communication and photographic purposes. Photos are deleted regularly in accordance with our data protection and privacy policies. They are tested before each trip by calling the nursery land line.

CCTV

- CCTV is in place to protect all staff and children. The content is automatically deleted after 2 weeks.
- We use closed circuit television (CCTV) as a way of helping keep children and staff safe as well as to protect our building. We also use it to support children and staff, and as a tool to reflect on risk benefit, accidents or injuries and issues as they arise.
- We follow the legal requirements that we are expected to meet under the Data Protection Act and promote best practice.
- We are mindful of individual rights and regularly assess whether this is the most effective way to keep people safe. We are mindful about the impact that CCTV could have on people's privacy. We take the protection of data seriously.
- We ensure our system operates within the law and have been taught how to use it for the purposes it has been designed to do. Parents and staff must send a written request for anyone not employed by the nursery to view the CCTV and this will be granted on a case-by-case basis, in line with GDPR and the Freedom of Information request. We maintain our membership of the Information Commissioners Office (ICO)

Walkie Talkies

- Walkie Talkies are allocated to all staff, and are stored in the office for charging at the end of the day and remain the responsibility of the allocated owner.
- They must not be dropped, thrown, placed in water, left outside or be unaccounted for at any time.
- They are not for children to use independently.
- Communication should be kept concise, factual, and professional.

Social Networking

- The Young Friends Kindergarten social media pages are monitored by a person with specific duty and roles and responsibilities to do so. Any images will follow

the Image Policy and specific permission gained from staff and parents for any recognisable image.

- Images gathered for social media will be taken with one of the nursery iPhones and the trip phone. These images will not show the faces of any children. The phones will be kept in the locked tech cupboard at night.
- Images are deleted regularly.
- The Social Hub social media page is for all staff and a safe space to learn and keep connected. Please refer to the Communication Policy for further guidance.
- All staff will maintain a professional identity on their social media, keeping personal information, political stances, and strong personal views away from their public profile. They must not have their place of work on any social media. Staff must never share online personal information (e.g., social networking profiles) with families. Families (personal and business profiles) either current or previous must not be friended, followed, or liked.
- Staff must not post anything derogatory about the nursery, post about the nursery day including sharing locations and never share any photos from the nursery on any group chat, thread, or individual post.
- Any post that is deemed to harm, airs a grievance, infers negligence or malice, is libellous or slanderous or in any way could be construed as defamation to the nursery or any staff member, will be treated seriously and may result in a professional discussion and further disciplinary procedures.
- Employees must be aware that their online behaviour could portray or reflect a political view, religious belief, personal standpoint, ideological challenge, extremist stance or cultural provocation that does not align with the nursery ethos or values and therefore could be deemed inappropriate
- All staff must be aware that if they or another member of staff are targeted online, for example online bullying or cyber bullying or harassment they should inform their line manager.
- Louise Lloyd-Evans or Emma Holmes will report online safety concerns to the Professionals Online Safety Helpline 0344 381 4772 helpline@saferinternet.org.uk
- All staff must check their privacy settings to make sure personal data is not being shared inadvertently or inappropriately and personal information is not being exposed. They must be responsible for managing their data securely online
- Staff social media pages are monitored for activity that affects the workplace, to protect staff and to ensure they are adhering to this policy
- When recruiting, we are obliged to check potential candidates online presence.
- All parents must adhere to the code of conduct as outlined on the Facebook Community Group.

Almas Finger-print System

- The Almas fingerprint system is in place to protect all children. Emma is responsible for ensuring fingerprints are recorded and only able to be used within working hours. Parents are not on the fingerprint system. Any staff without a DBS will not be added to the system.

Maintenance and Care

- All technology devices are labelled, and a list kept for keeping track of maintenance.
- PAT testing is carried out if required, for the purpose of stock taking and auditing resources. The Electricity at Work Regulations 1989 require that any electrical equipment that has the potential to cause injury is maintained in a safe condition. However, the Regulations do not specify what needs to be done, by whom or how frequently (ie they don't make inspection or testing of electrical appliances a legal requirement, nor do they make it a legal requirement to undertake this annually).
- All devices must be stored safely in an allotted place during each day out of the reach of children and in a lockable cupboard overnight.
- If any electronic devices break or are not working properly it is the staff member who finds its responsibility to alert a manager and fill out a form detailing what has happened if known. Whether known or unknown that person must inform their line manager who must inform management
- Management reserve the right to deduct the cost of an electronic device if it is broken or lost due to negligence of a team member.

External Links and Organisations

Portable Appliance Testing - [PAT \(Portable appliance testing\) - HSE's answers to popular questions](#)


Guide to the General Data Protection Regulation - [Guide to the General Data Protection Regulation - GOV.UK \(www.gov.uk\)](#)

Relevant Policies and Documents

GDPR Policy
Images Policy
Sustainability Policy
Communication Policy
Safeguarding Children Policy
Prevent Duty
Staff Code of Conduct
Parent Code of Conduct

Authorisation

Signature:



Louise Lloyd-Evans
Owner and Director

Young Friends Nature Nursery

89 Holland Road

Hove

East Sussex

BN3 1JP