The Use of Internet and Photographic and Recording Devices: Policy and Procedure:

Policy Statement:

The Service will ensure that the use of multimedia will be age appropriate and supervised when used.

Principle

Child Care Act 1991 (Early Years Services) Regulations 2016 (Síolta Standard 7: Curriculum, Síolta Standard 9: Health and Welfare) (National Standard 3: Working in Partnership with Parents or Guardians, National Standard 8: Care Play and Learning).

Policy and Procedure: Computers:

Computers are available to children in the Service.

Internet Access:

Children (School Aged Child Care) do have access to the internet.

They are fully supervised at all times while using the computer.

YouTube is strictly prohibited from being used in the service.

Mobile Technologies:

Staff are not permitted to use personal mobile phones when supervising children.

The taking of photographs on personal mobile phones is strictly prohibited anywhere in the service.

Children may not bring mobile phones, tablets, or similar devices into the Service Television/DVD:

Gaming Machines e.g. PlayStation, Nintendo Wii, Xbox:

Gaming machines are not used in the service.

Music & CDs:

At the Service we value music because it is a powerful and unique form of communication that can change the way children feel, think and act. It also

increases self-discipline and creativity, aesthetic sensitivity, and fulfilment. The CDs used are appropriate for young children and will contain no offensive or inappropriate language.

Spotify will be used for children's safe music.

Radios stations will not be listened to in areas where children can hear them as the content may not be suitable.

Music will not be played too loud so that the children's voices may still be heard.

Apps (Little Vista):

The school mobile phones are used strictly for reporting to parents/guardians on their child's day and NOT for personal use at any time.

• **The school mobile phones are to be used strictly for recording the children's details including**:

- Attendance
- Sleep checks
- Log daily activities
- Updates for parents/guardians
- Share photos with parents/guardians
- Developmental observations
- Aistear assessments

• Employees may with permission from Management use the school mobile phone to access the internet or email.

• Children may not use the school mobile phones at any time.

• Each staff member will have their own log in ID and this ID should not be passed to any other staff member at any time.

• The class mobile phones are to be used for signing in to work and signing out.

This will be used for Payroll and for Health and Safety purposes instead of sign in and out sheets.

• Each staff member must sign in for themselves and no other member of staff is permitted at any time to sign another member of staff in or out.

• These conditions must be strictly adhered to at all times and Disciplinary Policy will be invoked for any breaches of this policy.

Camera and Video Devices:

We are aware of the need for sensitivity when taking photographs and observe the following:

• Parental permission will always be sought before photos or videos are taken.

• Only the Service's tablet may be used to take pictures.

• Staff are not allowed to take pictures with phones/tablets or their own personal cameras. (If this is breached disciplinary action may be necessary).

• A photograph will only be taken if the child does not object to having his/her photograph taken.

• Photographs are used to show positive issues (e.g. a piece of work that the child has worked hard on or is pleased with, children playing cooperatively together etc.)

• We are inclusive so that gender, race, special educational needs and differing abilities are reflected in a balanced way.

• There may be cultural issues of which we need to be aware when taking photographs of children from different ethnic minority groups. Where photographs, videos or even samples of children's work are to be displayed outside the Service we seek parental permission for this to happen. Examples of this are newspaper reports, articles in early year's publications or exhibitions of children's work.

We will have written consent on our enrolment forms prior permission from parents/guardians for any images/videos collected that we would like to post on our website, Facebook or other social media. Students visiting professionals or researchers, who need to take photographs or videos as part of their work, are made aware of the need for confidentiality and that children will not be named or identified in any other way.

Further parental permission will be sought in this instance. Videos are also occasionally used in the Service for many of the above purposes. In particular we may use them for observations of children's play to further our understanding, or for assessment and planning tools. We will only use Netlfix or Disney Channel for the children to watch and all movies must be U rated.

Parents/Guardians Photographing and Videoing Children:

Parents/guardians may not take photographs or record children in the

Service without the consent of the Management Records:

The following records will be maintained:

• when a person can have access to a recording and photographic device

• in what circumstances

• for what purposes

• who can view, listen, or retain photographs/videos • in what

circumstances they can do this

• for what purpose Use of Photographs: Photographs are used throughout the Service for a variety of purposes.

Generally, Child Care practitioners take photographs of the children throughout the year to capture a particular example of play or something that a child has achieved. In addition, we use photographs for:

Photographs: Purpose:

- Staff will only take photos of the children while carrying out activities. • To share achievements with parents.
- For their learning folders.
- For the monthly time line to be displayed on their walls in the classroom.

Photographic or video recording will not be stored on devices in the Service for extended periods of time. If a photograph is likely to be used again it will be stored securely and only accessed by those people authorised to do so. We will not re-use photos more than one-year-old, without further permission from the subject of the photo or the parent, as applicable.

Social Media: Photographs posted on social media e.g. on the Service's closed Facebook page or on our website will be done with parents' consent.

Disposal of Photographs: In the event that we no longer require a photo it will be disposed of as confidential waste.

When photos are destroyed:

• The CD disk will be made unusable.

• The memory card / USB stick erased.

• The computer file deleted.

• Hard/printed copies and any negatives are shredded.

CCTV:

The system has been installed by the service with the primary purpose of ensuring the safety of children in our care, and helping to ensure the safety of all staff, parents/guardians and visitors consistent with respect for the individuals' privacy.

Data Controller:

Erika Deery is the designated Data Controller and they are responsible for the data/information collected using CCTV. Management is responsible for the operation of the system and for ensuring compliance with this policy.

This will be achieved by monitoring the system to:

• Ensure that children are appropriately cared for.

• Assist in the prevention and detection of crime.

• Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff and assist in providing evidence.

• Provide opportunities for staff training.

• To investigate accidents.

The system will not be used:

• To provide recorded images for the world-wide-web.

• To provide images for a third party, other than An Garda Síochána in the course of their enquiries.

• Daily monitoring of staff.

• Monitoring staff performance.

• A supervision tools.

• Recording any conversations.

NOTE: If after viewing the CCTV for one the reasons stated that any inappropriate practice or breach of policies is observed this would be brought to the attention of the employee, they would have the opportunity to view

same and depending on the matter this may result in invoking the discipline policy and procedure.

The Data Protection Acts of 1988 and 2003, and the 2016 General Data Protection Regulation (GDPR): CCTV digital images, if they show a recognisable person, are Personal Data and are covered by the Data Protection Acts. Location:

The following areas are currently monitored by CCTV

• External areas, front entrance hallway and all entry points. Fairness: Management respects and supports the individual's entitlement to go about his/her lawful business and this is the primary consideration in the operation of CCTV. Although there will be inevitably some loss of privacy with CCTV cameras are not used to monitor the progress or activities in the ordinary course of lawful business. They are used to address concerns, deal with complaints or support investigations.

- New employees will be informed immediately, at induction that a surveillance system is in operation.
- Parents/guardians will be informed when they enrol their child. They will be informed of the purpose of the CCTV and what it can and cannot be used to monitor.

Role of the Management:

• To ensure the system is always operational.

• To ensure that servicing and repairs are carried out as necessary to the system.

• To respond to any individual's written request to view a recording that exists of him/her or his/her children.

• To ensure prominent signage is in place that will make individuals aware that they are entering a CCTV area.

• To ensure that areas of privacy (toilets etc.) are not monitored using CCTV.

• To ensure confidentiality is maintained at all time. Recorded information will be stored in the office and will only be available to those directly connected with achieving the objectives of the system.

Copy/viewing Recordings:

Management will respond to a request to view a recording by allowing the viewing to take place, in the presence of management on the premises. This

is to protect other children/staff that may be present on the recording.

Copies of recorded information must be strictly controlled and only made in relation to incidents which are subject to investigation.

They must only be given to authorised third parties. Copies can only be issued by management.

Retention:

Recordings are retained for one month Access to Recordings: There is no obligation on the Service to comply with a request that it considers unreasonable or vexatious or if it involves disclosing identifiable images of third parties. Third parties must give consent. Recordings will however be provided, if required by law or authorised agencies such as the Garda.

• Requests for access to recordings must be made in writing.

• Sufficient information must be provided to locate the relevant recording, a specific date and reasonable time window.

• Viewings will take place, if appropriate, in the service in the presence of management.

• Management will have 21 days to respond.

• If a copy of recording is given to a third party that third party must sign a declaration form that they will not share the tape with anyone else, copy it or use it for unauthorized purposes.

• An incident report will be completed for each incident requiring investigation If access to or disclosure of the images is allowed, then the following should be documented:

1. The date and time at which access was allowed or the date on which disclosure was made.
2. The identification of any third party who was allowed access or to whom disclosure was made.
3. The reason for allowing access or disclosure.
4. The extent of the information to which access was allowed or which was disclosed. The identity of the person authorising such access.
5. Where the images are determined to be personal data images of individuals (other than the data subject) may need to be disguised or blurred so that they are not readily identifiable.

6. f. If the system does not have the facilities to carry out that type of editing, an editing company may need to be hired to carry it out. g. If an editing company is hired, then the Manager or designated member of staff needs to ensure that there is a contractual relationship between the Data Controller and the editing company.

Data Subject Access Standards:

All staff involved in operating the equipment must be able to recognise a request by data subjects for access to personal data in the form of recorded images by data subjects.

Data subjects may be provided with a standard subject access request form which:

a) Indicates the information required in order to locate the images requested.

b) Indicate that a fee will be charged for carrying out the search for the images.

c) The maximum fee which may be charged for the supply of copies of data in response to a subject access request is set out in the Data Protection Acts, 1988 and 2003.

d) Ask whether the individual would be satisfied with merely viewing the images recorded.

e) Indicate that the response will be provided promptly following receipt of the required fee and in any event within 20 days of receiving adequate information

Manager Signature:  Date: 20/07/2023