muddy boots
DAY NURSERY

E- Safety Policy and Procedures

Aims

- To be clear on the responsibilities of staff when using cameras, mobile phones, computers, and other electronic devices within the setting.
- To safeguard children's welfare in relation to the above areas and minimize the risk of harm.
- To fulfil legal duties in relation to personal data and other areas, e.g.: Data Protection Act 1998

Procedures

Digital and Video Images

- Written permission from parents/carers will be obtained and documented before any images of children are recorded. This may mean that separate permissions are needed for:
  a. Evidence of EYFS tracking or Play quality in the setting uploaded on Parents Portal.
  b. Use of images on setting website or Parents Portal.
  c. Images recorded during events/ parties/ fundraising or outings.

- Parents must be made fully aware of how any images of their children may be used or must have the right to decide if they wish their children to be photographed. Parents must be able to have a say in how these photos will be used.
- Digital images will be stored only on the nursery tablets. The tablets are kept only at nursery and never taken out of the setting. They get locked in the office at the end of the day.
- While using digital images, practitioners should be aware of the risk associated with taking, using, sharing, publishing and distribution of images.
- Nursery staff must only use the setting equipment: personal equipment must NOT be used to record images of the children.
- Staff should be vigilant when taking digital/video images of the children to ensure that they are appropriately dressed.
- Children's full names/names will not be used anywhere on the settings website or literature.
- Individual parent's wishes must be considered.
- After a photograph is taken down it will be either stored in the child's learning journal (Parenta), returned to the family or shredded (if printed).

Limited use of mobile phones and electronic devices

- Practitioners, volunteers, students etc will NOT have their private mobile phone on their person during work hours.
- Mobile phones will be kept in a secure area away from where the children are accommodated.
- Smart watches should be disconnected when in units.
- Personal laptops/tables should be used in office/staff room areas.
- Staff may use their mobile phones during their designated breaks and in an area away from the children.
- Nursery's contact number will be given as an emergency number in case practitioners need to be contacted.
- Nursery staff are not to use any mobile phone or any other electronic device/cameras to photograph the children.
- Visitors and parents will be asked to switch off their mobile phones or not to use phones while on the premises. If they need to use their mobile phone they will be asked to do so away from the children.
- If the setting is to be a mobile phone free zone a notice should be displayed outside to inform all visitors to the setting.

Use of mobile phones on outings

- Offsite on outings, mobile phones may be very useful. Where child information is stored on a personal mobile for an outing this needs to be deleted after the outing is over. It is recommended that the senior member of staff records this occurrence. Alternatively, paper information may be taken on outings.

- Setting practitioners must never exchange mobile phone numbers with children in their setting.
- Setting practitioners are not to use any mobile phone cameras to photograph the children.
- Practitioners will be held responsible for the content and security of their own phones, e.g. access to web pages. If this is deemed to be a safeguarding issue this will be dealt with in line with the settings child protection and disciplinary policy.
- Images taken of the setting or its children should be downloaded onto the settings computer/laptop/ tablet only. Images must not be downloaded onto any personal computer.

Smart watched used by staff

- Practitioners must disconnect their devices during working hours.

Computer, Laptop and Tablets

- Practitioners should not use the setting's computer/laptop/ tablets for personal use.
- The setting will ensure that all programs used, and websites accessed are appropriate and that children are not able to access or download material which is unsuitable.
- All setting files that contain personal data will be stored appropriately and securely, e.g.: password protected or locked away.
- Practitioners should not forward any of the settings work, files, information etc stored on the setting computer/laptop/ tablets to their home PC, unless this has been agreed by management as necessary practice for the setting. It is recommended that a log of "homework" should be kept in the setting and this needs to be checked and signed by management on a regular basis. Any work taken home needs to be appropriately protected as if it were in the setting and open to scrutiny by management.
- Practitioners should not use any personal memory devices in the setting's computer/laptop and tablets. Memory sticks provided by the setting should be used for work purposes only and should not be taken off the premises.
- If any ICT equipment is taken out of the building the manager/deputy must be informed.
- Practitioners should not access, copy, remove or otherwise alter any other user's files, without their expressed permission.
- All email communication should be appropriate and written in a professional manner.
- E-mail attachments should only be opened if they are from a source known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- Illegal or inappropriate materials MUST NOT be uploaded, downloaded or accessed.
- Practitioners should ensure that setting's computer/laptop and tablets is used appropriately to avoid disabling or damaging equipment.

Social Networking Sites

- Practitioners, volunteers, students, registered bodies etc should not put details of their work on any form of social networking site.
- Practitioners, volunteers, student, registered bodies etc should not engage in any on-line activity that may compromise their professional responsibilities.
- Photographs, names of, or comments about children within the setting must never be placed on any social networking site.
- Adults working with children should not correspond with setting's children/families through social networking sites.
- Practitioners should be aware of possible implications when entering any personal details on any gaming or social networking sites (e.g. YouTube, Facebook, twitter etc).

- The setting's computer, laptop and tablets should only be used for setting related activities. Practitioners will not be permitted to use the equipment to access social networking sites at any time, including designated breaks.
- All communications in the setting should be transparent and open to scrutiny.
- All staff should be made aware that failure to comply with policies and procedures may result in disciplinary action being taken.
- Parents will only use nursery contacts to pass on information in reference to their child or nursery – please contact us by telephone 0117 9684493 or email nursery@trinitycollegebristol.ac.uk

Responsibilities

This means that adults should:

- Report any concerns about any inappropriate or intrusive photographs found or any activity that raises concerns.
- All staff should be made aware that failure to comply with policies and procedures may result in disciplinary action being taken.
- Be aware that not following club guidance is potentially a child protection issue which may affect their suitability to work with children.

Further Information

South West Child Protection Procedures – provide detailed online information on all aspects of child protection – www.swcpp.org.uk

Guidance for Safer Working Practice for Adults who work with Children and Young People - DCSF www.dcsf.gov.uk/everychildmatters/resources-and-practice/IG00311/

Data Protection www.ico.gov.uk

Reviewed on:	Reviewed by:	Next Review:
November 2025	Silviya Velikova (Deputy Manager)	November 2026