



Safeguarding and Welfare Requirement: Child Protection

The safeguarding policy and procedures must include an explanation of the action to be taken in the event of an allegation being made against a member of staff, and cover the use of mobile phones and cameras in the setting.

1.6 Online Safety, Mobile Phones, Cameras and Electronic Devices

Policy statement

At **Impact Montessori Nursery**, we recognise that technology forms an important part of children's lives and can support learning, communication, assessment and the effective running of the nursery.

We are committed to protecting children, young people and vulnerable adults from inappropriate or unsafe use of technology, the internet, mobile phones, cameras, smartwatches and other electronic devices.

We will ensure that:

- technology is used safely and appropriately;
- children are appropriately supervised when using digital devices;
- personal devices are managed in accordance with our safeguarding procedures;
- photographs and videos of children are taken only for legitimate purposes and with appropriate consent;
- children's personal information and images are stored and shared securely;
- staff maintain appropriate professional boundaries online; and
- any online safeguarding concern is reported, recorded and dealt with in accordance with our Safeguarding and Child Protection Policy.

This policy applies to all staff, volunteers, students, agency staff, contractors and visitors.

1. Designated responsibility

Our **Designated Safeguarding Lead (DSL)** has overall responsibility for online safety and for coordinating any safeguarding concerns relating to the use of technology.

DSL: _____

Deputy DSL: _____

The DSL will ensure that online safety arrangements are reviewed regularly and that staff receive appropriate information and training.

2. Nursery ICT equipment

- Only authorised nursery devices and equipment may be used by children.
- Nursery devices must be password protected where appropriate and kept securely.
- Devices must have appropriate security, privacy and virus protection.
- Appropriate filtering and safety settings will be used where children have access to the internet.
- Staff must not download unauthorised software or applications onto nursery devices.
- Staff must not use nursery devices for inappropriate, illegal or unauthorised purposes.
- Nursery devices must be kept secure when not in use.
- Any loss, damage, security concern or suspected data breach must be reported to the manager immediately.
- Before a second-hand or donated device is used, it must be checked and securely cleared of inappropriate or personal material.

3. Children's use of the internet and digital devices

Children will only access the internet when this forms part of an appropriate learning activity.

- Children will never have unsupervised access to the internet.
- Staff will check websites, applications, videos and online resources before using them with children.
- Age-appropriate resources will be selected.
- Children will not be permitted to access social networking sites.
- Children will not be permitted to make purchases or enter payment details online.
- Voice-activated searches and other technology that may produce unexpected content will be appropriately supervised.
- Staff will model safe and responsible use of technology.
- Screen use will be purposeful, proportionate and appropriate to the child's age and stage of development.
- Staff will ensure that digital activities do not replace children's opportunities for interaction, play, physical activity and adult engagement.

Current EYFS guidance requires providers to have regard to screen-use guidance and emphasises proportionate use of digital devices. [Help for Early Years Providers+1](#)

4. Teaching children about online safety

Online safety will be introduced in an age-appropriate way through children's learning and personal, social and emotional development.

Children will be encouraged to understand simple messages such as:

- Tell a trusted adult if something online worries or upsets you.
- Be kind and respectful when using technology.
- Keep personal information private.
- Ask an adult before using something you do not understand.
- Do not send or share photographs without permission.
- Do not communicate online with people you do not know.

- Remember that adults can help if something online feels wrong.

Staff will support children to develop confidence in talking about anything that makes them feel uncomfortable or unsafe.

5. Staff use of mobile phones

Personal mobile phones must not be used while staff are working directly with children.

- Personal mobile phones must be switched off or placed on silent and stored securely in the designated staff storage area.
- Staff must not carry personal mobile phones in pockets while working with children.
- Staff must not make or receive personal calls or messages while supervising children.
- Staff must not use personal phones to access social media while working.
- Staff must not use personal phones to photograph, video or record children.
- Staff must not use personal phones to store children's photographs, videos or personal information.
- In an emergency, a personal mobile phone may be used with the manager's permission and, wherever possible, away from children.
- Staff on outings may carry an authorised phone for emergency purposes, but it must not be used to take personal photographs or for personal communication.

Any breach of this procedure will be treated as a safeguarding concern and may result in disciplinary action.

6. Children and visitors using mobile phones

Children should not bring personal mobile phones, tablets, smart devices or other electronic devices into the nursery unless there is an agreed individual arrangement based on the child's needs.

If a child brings a device into the nursery, it will be stored securely and returned to the parent/carer at collection.

Parents, carers and visitors are asked not to use mobile phones or cameras while on nursery premises.

Where a visitor needs to make an essential call, they will be asked to use the phone away from children where possible.

7. Cameras and photography

The nursery may take photographs or videos of children for legitimate purposes such as:

- recording learning and development;
- maintaining children's learning journals;
- documenting activities and experiences;
- displays within the nursery; or
- agreed nursery publicity.

Before photographs or videos are taken:

- appropriate parental/carer consent must be obtained;
- staff must ensure that the image has a legitimate purpose;
- only authorised nursery equipment should be used;
- the number of photographs and videos taken should be kept to a minimum;
- images must be stored securely; and
- images must only be shared using approved and secure systems.

Current government guidance specifically recommends keeping children's images and videos to a minimum and sharing them with parents through technically secure methods. [Help for Early Years Providers](#)

Staff should also seek the child's cooperation and, where developmentally appropriate, ask permission before taking their photograph.

8. Personal cameras and recording equipment

Staff, volunteers, students and visitors must not bring personal cameras or other recording equipment into areas where children are present for the purpose of photographing or recording children.

This includes:

- mobile phones;
- tablets;
- digital cameras;
- video cameras;
- wearable cameras; and
- other devices capable of taking or storing images.

9. Smartwatches and wearable technology

Impact Montessori recognises that smartwatches and wearable devices may have useful functions. However, some devices can receive messages, access the internet, record audio or images, or communicate with other devices.

To safeguard children:

- Staff must not use smartwatches to make or receive calls, read messages or access social media while working with children.
- Smartwatches must not be used to take, access or share photographs or videos of children.
- Where possible, smartwatches should be placed in flight mode or have communication functions disabled while staff are working with children.
- Staff must not use wearable devices to record conversations or audio involving children.
- Staff must not access personal notifications while supervising children.
- The manager may require a staff member to remove or securely store a smartwatch if its functions present a safeguarding or distraction risk.
- Any smartwatch or wearable device with imaging or sharing capabilities will be managed in accordance with this policy.

The current EYFS safeguarding framework specifically covers mobile phones, cameras and **other electronic devices with imaging and sharing capabilities**. [Help for Early Years Providers](#)

10. Electronic learning journals

Where an electronic learning journal is used:

- the system must be approved by the nursery;
- appropriate parental consent must be obtained;
- staff must use individual authorised logins;
- passwords must be kept confidential;
- information must only be accessed by authorised users;
- photographs and information must only be uploaded for legitimate purposes;
- staff must check that photographs are being uploaded to the correct child's record;
- information must not be downloaded onto personal devices unless specifically authorised;
- staff must not share login details; and
- any suspected breach must be reported immediately to the manager.

The nursery will ensure that online learning journals and digital assessment systems are used in accordance with data protection and security requirements. GOV.UK+1

11. Email and electronic communication

- Staff must use authorised nursery email accounts and systems for professional communication wherever possible.
 - Staff must not communicate with children using personal email accounts.
 - Staff must not use personal email or messaging accounts to communicate privately with parents about nursery matters unless specifically authorised.
 - Confidential information must only be shared through secure and appropriate methods.
 - Personal information must never be sent to the wrong recipient.
 - Staff must check email addresses and attachments carefully before sending confidential information.
 - Staff must not forward confidential nursery information to personal email accounts or personal cloud storage.
-

12. Social media and professional boundaries

Staff are expected to maintain professional boundaries both online and offline.

Staff must:

- maintain appropriate privacy settings on personal social media accounts;
- not accept current parents/carers or children as personal social media contacts;
- not communicate privately with children or parents through personal social media accounts;
- not share photographs or information about children;
- not post confidential information relating to the nursery, children, families or colleagues;
- not post comments that could bring the nursery or its service users into disrepute;
- not discuss safeguarding, complaints or individual children online;
- report inappropriate online contact or concerns to the manager/DSL.

If a staff member already has a personal relationship with a family before the child joins the nursery, this must be disclosed to the manager so that appropriate professional boundaries can be agreed.

Staff should remember that online information may be copied, shared or accessed by others even where privacy settings are used. Government online-safety guidance also highlights the importance of managing staff digital reputation and professional boundaries. GOV.UK+1

13. Inappropriate or harmful online material

Staff must report immediately if they become aware of:

- inappropriate or harmful material being accessed by a child;
- online bullying;
- grooming or inappropriate online contact;
- sexual exploitation or abuse online;
- inappropriate images involving children;
- extremist or terrorist material;
- racist, discriminatory or abusive online content;
- attempts to obtain personal information from a child;
- a member of staff behaving inappropriately online; or
- any other online activity that may place a child at risk.

The concern must be reported to the DSL and recorded in accordance with the **Safeguarding and Child Protection Policy**.

Where appropriate, concerns will be referred to the police, children's social care, Ofsted or another relevant agency.

14. Inappropriate images

Staff are reminded that making, possessing or distributing illegal images of children is a serious criminal offence.

If staff become concerned that a colleague, visitor or another person is:

- taking inappropriate photographs;
- requesting inappropriate images;
- storing or sharing inappropriate images;
- communicating inappropriately with a child online; or
- attempting to groom a child online,

they must report the concern immediately in accordance with the nursery's **Safeguarding and Child Protection Policy and Allegations Against Staff Procedure**.

Staff must not attempt to investigate the matter themselves or confront the person concerned unless instructed to do so by the appropriate safeguarding or law-enforcement authority.

15. Online bullying

If a child or family reports online bullying or harmful online behaviour:

- the concern will be taken seriously;
 - the DSL will be informed;
 - the concern will be recorded;
 - parents/carers will be involved where appropriate;
 - the child's wellbeing and safety will be considered; and
 - appropriate safeguarding advice and support will be provided.
-

16. Data protection and information security

All staff must comply with the nursery's data protection and confidentiality procedures.

Personal information, photographs and videos of children must:

- only be collected where there is a legitimate purpose;
- be accessed only by authorised people;
- be stored securely;
- not be transferred to personal devices;
- not be shared through unauthorised apps or messaging services; and
- be deleted or disposed of securely when no longer required.

Any suspected loss, unauthorised access or disclosure of personal information must be reported to the manager immediately.

17. Online safety training

All staff will receive information and/or training on online safety as part of their induction and through regular safeguarding updates.

Training will include:

- safe use of mobile phones and cameras;
- smartwatches and wearable technology;
- online safeguarding risks;
- professional boundaries and social media;
- appropriate use of nursery devices;
- data protection;
- recognising online abuse and grooming;
- reporting concerns; and
- maintaining children's privacy and confidentiality.

The DSL will maintain up-to-date knowledge of online safeguarding risks and guidance.

Current government guidance recommends regular online-safety training and ensuring that staff know how to report and escalate concerns. GOV.UK

18. Monitoring and review

The manager and DSL will monitor compliance with this policy.

Any breach will be considered and may result in:

- additional supervision or training;
- removal of access to devices or systems;
- disciplinary action;
- referral under safeguarding procedures; or
- referral to external agencies where appropriate.

This policy will be reviewed at least annually and following any significant incident, technological development or change in statutory guidance.

Legal and guidance framework

This policy is informed by:

- Early Years Foundation Stage (EYFS) Statutory Framework, effective from 1 September 2026;
- current Department for Education guidance on safeguarding and online safety;
- UK Council for Internet Safety guidance for early years settings;
- Data Protection Act 2018 and UK GDPR;
- Working Together to Safeguard Children 2026; and
- relevant Ofsted requirements and guidance.

Useful guidance

- Department for Education – Early Years Foundation Stage statutory framework
 - UKCIS – Online safety guidance for early years settings
 - Help for early years providers – Screen use
-

Policy approval

This policy was adopted by: Impact Montessori Nursery

Date adopted: _____

Date of next review: _____

Signed on behalf of the provider: _____

Name of signatory: _____

Role: Nursery Manager

Signature: _____

Date: _____

