



Developing a Mobile phone, cameras and other electronic devices with imaging and sharing capabilities.

Providers must take all necessary steps to keep children safe and well – Statutory Framework for the Early Years Foundation Stage 2024 - Children learn best when they are healthy, safe, secure, when their individual needs are met. (GP 3.1 & CM 3.1)

The procedure should include:

- How consent is gained from parents before images of children are taken, used & stored.
- The importance of settings being clear as to why they are taking images and for what purpose, for e.g.
 - Advertising
 - To demonstrate good practice.
 - To share information with parents
 - As evidence to Ofsted
 - Displays within the setting.
 - Children's observations & assessment files.
 - Social Media
- This section should also include information regarding what will happen to the images once the activity they are being used for has been concluded
- Consent that is required from parents where their child may be included in a photograph within another child's learning journey
- Systems that are in place where settings may invite a commercial photographer into the setting, including suitability checks, that they are a registered photographer and that they are appropriately supervised.
- How staff should report concerns if they find any inappropriate or intrusive images and the process for this. Where inappropriate photographs are identified the safeguarding and child protection policy must be followed.
- How the setting will ensure that any images will not cause any anxiety, distress or offence to the child and/or their family.
- Where all parental authorisation forms will be stored once authorisation has been sought and who holds the responsibility to ensure that happens.
- What situations may occur when extra parental permission may be sought, i.e. student and work placements, Christmas parties and external agencies etc. Further meetings should be organised between setting and parent where additional consent is required for taking images and prior arrangements that should take place
- How all consent records will be monitored and kept updated regularly and by whom.

- How the setting maintains confidentiality (Refer to the confidentiality policy) and adheres to the Data Protection Act (DPA) 2018 and the General Data Protection Regulations 2018
- How practitioners ensure that photographs are not taken of any children who may be in vulnerable circumstances, for example, children who may be in care or children who may be at risk of significant harm. If a child is in public care (looked after) the authorisation on the parents behalf must come from the child's social worker
- Ensure that the only device i.e. camera, mobile phone, iPad to take images or videos of the children is the device provided by the setting.
- Childminders taking photographs & videos on personal phones should be aware of the implications of this i.e. is the phone password protected? who has access to the phone? how long are images stored?
- For childminders, what is the procedure for your own families use of devices around childminding children.
- How do you ensure that staff or assistant do not use their personal phones during working hours, how is this managed if staff are allowed their phones during breaks and on outings.
- What is the procedure around smart watches.
- The procedure to follow should staff or parents/carers wish to take photographs of their own child.
- What is the procedure around mobile phones and smart watches when visitors or parents come to the setting.
- What is the procedure for allowing children to bring their own mobile phones, smart watches, laptops, consoles etc. to the setting.
- How people are made aware that mobile phones or personal cameras should never be used to take images of children.
- The procedure the setting follows once photographs have been taken, how these are printed and who holds the responsibility to ensure that all printed and unused photographs are deleted from the camera's memory. Images should never be stored in personal computers.
- How a group photograph of all children involved in an outing will be taken on the day, in order to support a potential critical incident, i.e. should a child be abducted or go missing, practitioners will be able to use the photograph to identify some personal characteristics about the child, for e.g. the clothes the child was wearing
- Where a setting has a Social Media page, it is strongly advised that this be a 'closed Social Media account' where images of children are shared, this good practice will support effective management of the page. Are parents aware of the group and know whether this is an open or closed account.
- Children should always be appropriately dressed when participating in activities where practitioners may be taking photographs.

- Photographs or any other imaging should never take place during intimate care routines by any person, including visitors, staff, parents or outside agencies.
- If the setting has CCTV including a Ring doorbell, how are parents made aware of this? It is advised that a sign is displayed to notify them this is in place and whether it is visual or auditory. This should outline who has access to the footage and how long it is stored for.
- **N.B. Where settings keep electronic records on children and families they must be mindful of their responsibilities under Data Protection Act (DPA) 2018 and the General Data Protection Regulations 2018**
- **Certain records will result in the setting needing to register with the Information Commissioners Office (ICO). This includes where settings take digital photographs of children – The notification helpline number for the ICO is 0303 123 1113**

To comply with the EYFS 2024 and the General data Protection Regulations (GDPR 2018)

- Specific parental; permission is requested, in writing before images of children are taken.
- Parents are informed about their right to withdraw their consent.
- Ensure staff/students and volunteers are trained in the safe use of images.
- Visitors are supervised on the premises and image recording equipment is not used.
- Photos are deleted off devices when no longer required.

Concerns about inappropriate taking or using of images must be immediately reported to the Designated Lead in the setting. Data Breaches will be reported without delay to the ICO and affected parents will be informed.

The procedure must be reviewed:

- At least annually.
- The procedure needs to be signed by the registered person, include reviewed date and the next review due date.
- If any changes are made to the procedure when reviewed the staff and/or parents need to be informed.

This information is provided for guidance only. It is your responsibility to ensure that all statutory legal guidance is adhered to. Consideration needs to be given to any changes in legislation subsequent to the production of this information.