



Confidentiality policy

Rationale

In order to fully cater for children's individual needs and abide by the requirements of the Early Years Foundation Stage (EYFS) and the Childcare Register, I need to obtain personal information from parents/carers about their child. I respect parents/carers' privacy and request that parents/carers and children respect mine and my family's confidentiality.

Information will only be used to enhance the welfare of the children in my care and that any information collected will be stored to retain confidentiality according to the GDPR (General Data Protection Regulation) 2018 and UK's Data Protection Bill 2018.

Procedure

Storage of personal information

The GDPR requires me to keep and use all information in a safe and secure way. Confidential records are stored electronically in a password protected form. Any information or photographs that are stored on my computer will be protected by a strong password or biometrics, firewall and virus checker. I have registered with the Information Commissioner's Office (ICO) as a Data Controller.

Usage and sharing of personal information

Both written and verbal information gained about children and their families will be treated as confidential and not shared without parents/carers' permission unless legally required to do so, for example to safeguard a child, to support a child with allergies or to work in partnership with another setting that a child attends. Sensitive conversations with parents/carers will be conducted outside the hearing of other parents/carers – this may be through an arranged meeting or phone call if not possible when child is collected.

To comply with my legal responsibilities, written information will be shared with Ofsted if requested. This can happen as part of an inspection or at any other time there is a reason for Ofsted to inspect it. Any requests for personal information

regarding minded children or families by other parents/carers, childminders or members of the public will be strictly denied.

Data breaches

In the event of a data breach, (ICO describe a data breach as 'A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'.) I will keep a record of the breach, and the actions taken to rectify the situation and to prevent it happening again. If it is a risk that is severe enough to risk to people's rights and freedoms I must notify the ICO within 72 hours. To comply with GDPR parents would be informed of any breach of their data.

Data retention

Written information will be kept after a child leaves, for the amount of time stipulated by Ofsted, the ICO and/or the setting's insurance provider before being securely destroyed. A list of retention periods for different types of documentation is available upon request.

Data Subject Access Requests (DSARs)

Parents have the right under the GDPR to see any record of information kept about their child. You can ask to see your child's records at any time or requests can be made in writing and I must provide the relevant access within 1 month. The only exception to this will be for information that is exempt (For example, information such as some child protection records that would not be in the child's best interests to provide). To comply with the GDPR there will be no charge for this.

CCTV, mobile telephones, smart devices and recorded images

Our home is protected by internal and external CCTV Cameras and by a video-capture doorbell. Videos captured may be stored and saved for a maximum period of 10 days in secure cloud storage. In order to access my account, I have enabled two factor authentication meaning a password and security code is needed to log in which helps prevent the account being hacked. Videos of minded children and their families will not be shared without permission, apart from for safeguarding reasons or if requested by Police.

My personal mobile phone is used as my main setting phone. It is the only phone permitted to take photographs and videos of childminding children. Other family members are not permitted to take photographs, videos or recordings of children within my childminding setting using any device, including but not limited to mobile phones, cameras, smart watches or other devices capable of taking images.

In line with ICO requirements, you can request to see any images held at any time. I will only be able to show you images and recordings where no other individuals are visible. You can request for recorded images of your child to be deleted and these must be deleted within one month, unless needed for safeguarding reasons or legal dispute.

Outside of the setting

From time to time we may visit places where there is CCTV, or where other people are taking photographs, such as playgroups, care homes, or public places such as parks and natural spaces. We are unable to control any images or recordings taken in these places.

Artificial Intelligence ('AI')

We will not knowingly share images, recordings or personal information relating to a child with AI, for example ChatGPT, Gemini, Claude or Grok.

Personal and confidential information relating to me and my family

It is likely that you will also find out confidential information about my family through conversation and from spending time in my home. I request that you treat this information as confidential and not share with others without permission.

Signature: Meg Hearne

Date: 05 June 2026