

Nottinghamshire County Council

Policy Library Pro Forma

This information will be used to add a policy, procedure, guidance or strategy to the Policy Library.

Title: Taking Photographs with Mobile Devices

Aim / Summary: To provide guidance for staff who need to take photographs with their NCC issued mobile devices

Document typ	e (please choose one)		
Policy		Guidance	Х
Strategy		Procedure	

Approved by:	Version number: 1
Date approved:	Proposed review date:

Subject Areas (choose all relevant)				
About the Council		Older people	Х	
Births, Deaths, Marriages	Х	Parking	Х	
Business	Х	Recycling and Waste	Х	
Children and Families	Х	Roads		
Countryside & Environment	Х	Schools		
History and Heritage	Х	Social Care	Х	
Jobs		Staff	X	
Leisure		Travel and Transport	Х	
libraries				

Author:	Responsible team:
Contact number:	Contact email:

Please include any supporting documents		
1.		
2.		
3.		
Review date	Amendments	



Taking Photographs with Mobile Devices - Staff Guidance

Contents:

1.	Introduction	. 2
	Taking photographs of other organisation's records or case notes	
3.	Taking Photographs of supporting evidence	. 3
4.	Taking photographs of a person or their home	. 3
4	4.1. Publicity and marketing	. 4
	Taking photographs at incident / accident locations or for evidence purposes	
6.	Storage of images	. 4
	6.1. Disposal of images	

1. Introduction

The introduction of corporate mobile devices means that staff now have easy access to a camera, which can be used for work purposes, for example, taking photographs of:

- Records or case notes relating to a named person;
- A person's home (inside or outside);
- A person;
- An incident / accident location or property;
- Or for the purpose of recording an event or activity.

NOTE: you should only do this where it is needed as part of your work, it does not cover every possible scenario and you should consider whether a photograph is the best way to capture the information you need.

The Data Protection Act applies where photographs are taken and stored with personal details such as names and addresses. The purpose of this guidance is to make sure that staff act within the law if they take and store photographs of this kind.

The guidance applies to thinkpads, cameras, mobile phones, videos and any other equipment capable of recording images. Any reference to photographs and photography should be interpreted as including filming/ videography.

Staff should be aware that the use of personally owned devices may not be used for these purposes except in the case of an emergency where there is risk of harm.

2. Taking photographs of other organisation's records or case notes

Photographs may be taken of records, risk assessments and case notes. Verbal permission to do this must always be sought from, for example, the relevant NHS or care home manager, in the same way that a staff member might request a photocopy of relevant documents. If photographs of this kind are taken, they should be captured within the Total Mobile application or if this is not possible they must be uploaded into the relevant corporate system and deleted from the mobile device within 1 working day.

3. Taking Photographs of supporting evidence

Where photographs of identification or financial documents are taken to support a service user's application for services to be provided these should be treated in the same way as records or case notes from other organisations.

4. Taking photographs of a person or their home

When taking or using photographs of a person or their home, staff must respect the person's privacy and dignity, and their right to make or participate in decisions that affect them. This means that staff must:

- Give the person(or their representative / parent/ guardian) information about the purpose of the photograph;
- Ask the "person's" (or the parent/guardian in the case of a child) permission to take the photograph;
- Make sure that the person does not feel under pressure to have the photograph taken;
- Where the photograph is to evidence a safeguarding concern, care should be taken to ensure that the photograph accurately reflects the situation.

If there are any doubts about a person's ability to make a decision about having their photograph taken, the person taking the photograph must determine whether it is in the person's best interests to go ahead. A written record of the "best interest decision" should be placed on the case file.

The photograph must be deleted if the person requests it.

Where a personal device (as distinct from a Council one) is used due to risk of harm the image should be shared with appropriate services (e.g. police) and emailed to an appropriate council email address immediately so that it can be transferred to the record.

If the photograph is taken for safeguarding purposes, particularly in relation to children or vulnerable adults, then consent is not necessary and the photograph should be kept on the appropriate case record. The photograph must not be used for any other purpose.

Page: 3

4.1. Publicity and marketing

Images for use in leaflets, videos or other media must be accompanied by signed consent forms, see <u>Using photos</u>, video and audio for further information. On no account must photographs of people ever be shared on social media. See the Council's <u>Social Media Policy</u>.

5. Taking photographs at incident / accident locations or for evidence purposes

Photographs may be needed to provide evidence in support of the council's position in a legal (e.g. health and safety or safeguarding), regulatory or disciplinary process. These should be treated in the same way as case notes or records and uploaded to the appropriate system or file location within one working day and then removed from the device, especially if these photographs contain images of people.

6. Storage of images

Images stored on a tablet or other mobile device must be uploaded into the relevant corporate system within 1 working day, and a note recorded in case notes as applicable. They must then be deleted from the tablet/ mobile device immediately

6.1. Disposal of images

Photographs that are out of date or no longer usable must be destroyed appropriately by deletion of the electronic record or by being archived in line with the Data Protection Act.