



ASTON ON TRENT PRIMARY SCHOOL



PHOTOGRAPHIC IMAGES OF CHILDREN


**Reviewed without amendment by Governors
Resources Committee on 13 November 2023**

**This policy has been impact assessed in the light of
all other school policies, including the Disability
Equality Scheme.**

Minute No: 54/23R

Signed:  **Print Name: C Jones**

Date: 13th November 2023

Signed:  **Print Name: S Moore**
Date: 13th November 2023

Derbyshire County Council Image Use Guidance and Template Policy for Educational Settings

V01

June 2018

Contents

Contents

Contents	3
Introduction	4
Frequently Asked Questions for Educational Settings	5
Supporting Advice and Guidance.....	16
Children’s Images: Frequently Asked Questions for Parents/Carers	32
Template Letters and Forms.....	Error! Bookmark not defined.
Useful contacts and Links	Error! Bookmark not defined.
Acknowledgement.....	34

Introduction

The use of images guidance and policy template applies to the use of all film and electronic photographic equipment; including cameras, mobile phones, webcams, tablets and portable gaming devices with inbuilt cameras, as well as other forms of digital technology and resources for storing and printing images.

As cameras and personal devices have become more advanced and easier to use, it is increasingly likely that children and their families will be using photography as part of everyday family life. All educational settings must therefore consider the impact such technology may have.

Whilst it brings significant benefits, digital technology has increased the potential for cameras and images to be misused; inevitably there will be concerns about the risks to which children and young people may be exposed. Educational settings however must be aware that the behaviours of individuals using the technology present the risk, not the technology itself.

Educational settings will need to amend and adapt the sample materials included in this document according to their ethos and the technology available.

In developing a policy for your own educational setting, we suggest that head teachers, managers, Data Protection Officers (DPOs), Designated Safeguarding Leads (DSLs) governing bodies and other leadership staff should open the issue for discussion and explanation with parents/carers and other stakeholders. Any parents/carers and staff members with particular concerns must always be able to withhold their consent for image use for whatever reason.

This guidance document and policy template is suitable for educational settings including (but not limited to) schools, early year's settings, Pupil Referral Units, 14-19 settings, further education colleges, alternative curriculum provisions, Children Centre's and hospital schools etc. We encourage all education establishments to ensure that their policy is fit for purpose and individualised for their context. For simplicity we may use the terms 'school' and 'pupils' or 'pupils' within this document, but stress that its use within other educational settings and beyond are relevant and appropriate although it will require adaptation to meet the needs of specific communities, ages and abilities.

Please be aware that legislation may be updated on a national and international level, therefore this guidance is subject to constant review. Settings must ensure that they take responsibility for keeping their policy and practice up-to-date.

Frequently Asked Questions for Educational Settings

Why do we need an image policy?

Schools, nurseries, playgroups and youth groups have always used photographs as a way of celebrating achievements or seeking publicity for fundraising etc. Parents, families and the children themselves often enjoy seeing their loved ones in print or on a website. We want to ensure that everyone can continue to enjoy these activities safely.

However all members of the community need to be aware that placing any identifying information in the public domain has risks as well. Parents/carers specifically will need to understand these issues to give properly considered consent. It is also important that parents and settings can fully consider the issues before any problems arise.

Section 3.4 of the statutory framework for the Early Years Foundation Stage (EYFS) identifies that "...safeguarding policy and procedures must ... cover the use of mobile phones and cameras in the setting". All settings with foundation stage provision must therefore have a policy which covers the use of mobile phones and cameras. It is however advisable that all educational settings ensure appropriate policies and procedures are in place as part of safeguarding and data protection practice.

Educational settings will also have statutory obligations to ensure use of images complies with data protection legislation; this includes the General Data Protection Regulation (GDPR), and any other relevant Data Protection legislation.

What are the risks?

The most highly publicised and worrying risk is that a child who appears in the paper or on a website may become of interest to a sex offender. Locating people through the internet has become extremely easy, using widely available software, so if there is a picture and the name of a school, setting or youth group and the full name of the child or adult then it could be quite easy to find out someone's exact location or address which could then put them at risk.

There are also other specific groups of children, families and staff whose safety could be put at risk if identified e.g. families fleeing domestic violence. Educational settings may not always be aware of who these vulnerable groups may be. Designated Safeguarding Leads (DSLs) within educational settings will have a crucial role to play in ensuring that image use takes place in line with safeguarding expectations.

Most children who suffer abuse are abused by someone they know. We have taken the view, in consultation with the local police force, that the risk of a child being directly targeted for abuse through being identified in an image by a

stranger is small. By taking reasonable steps to ensure photography is appropriate, and that personal information is protected, photography for setting and at other events by staff, families and the media should be allowed. Due to the widespread use of devices with built in cameras, a total ban would be very difficult for settings to impose and to enforce. Photographs are a source and pride for educational settings, children and young people and their families; this should continue within safe practice guidelines.

Isn't this just scaremongering?

Sadly not. There have been cases of families and staff receiving unwelcome phone calls or visits following appearances in the press or on an educational settings website or social media channel. However, this is rare, so it is important to have a sense of proportion. Educational settings will want to celebrate success and achievement, but parents/carers must be aware of risks to make informed decisions.

Whilst ultimate responsibility for abuse lies with perpetrators, a staff culture which is complacent (e.g. believe that abuse “couldn’t happen here”) and unclear can facilitate an environment whereby abuse is not recognised, which can place children at significant risk of harm. Clear and understood boundaries regarding safe and appropriate use ensures all members of staff can identify and challenge poor practice. A culture with clear expectations for safe and responsible use of personal devices, enforced by an informed and aware management is essential.

What do leaders need to consider?

Educational setting leaders and managers should ensure that the settings policy covers specific expectations for safe and responsible use for mobile phones and personal devices by children, staff and others. Such policies should cover the wide range of devices with built in cameras available, such as tablets, phones, smart watches etc. The image policy should apply to and be understood by all individuals who have access to or are users of work-related photographic equipment. This will include children, parents and carers, staff and their managers, volunteers, students, committee members, visitors, contractors and any other community users.

The leadership team is ultimately responsible for ensuring the acceptable, safe use and storage of all technology and images. This includes the management, implementation, monitoring and review of the setting’s Image Policy. The manager, head teacher, DPO and/or DSL can reserve the right to view any official images taken and can withdraw or modify a member of staffs’ authorisation to take or make official images at any time. All members of staff must ensure that all images are available for scrutiny and be able to justify any images in their possession.

Does the Government have a policy for educational settings on the use of photographs?

No. The following was posted on the DfE Website in 2012:

"No, schools and local authorities are free to decide on their own policies relating to the use of such images or the release of associated information for their own publicity purposes. We do, however, advise that photographs and video images of pupils and staff are classed as personal data under the terms of the Data Protection Act 1998. Therefore using such images for school publicity purposes will require the consent of either the individual concerned or in the case of pupils, their legal guardians."

Further guidance can be obtained from the Information Commissioners Officer at: http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx

Derbyshire County Council's 'Access your Information' content can be found at: <https://www.derbyshire.gov.uk/working-for-us/data/gdpr/access-your-information/access-your-information.aspx>

Do we have to pay a fee to the ICO?

Data Controllers are people or organisations who process personal information. If you collect and store personal data about the children you look after and their parents or carers, you must comply with the GDPR and the Data Protection Act; in particular the 6 principles.

Data Controllers must pay the ICO a data protection fee unless they are exempt. There are three different tiers of fee and controllers are expected to pay between £40 and £2,900 depending on amongst other things, your annual turnover and the number of staff you have.

Generally speaking you have to pay a fee if you are processing personal information, but there are some exemptions. Data controllers who are exempt from paying a fee must still comply with the other provisions of the Act.

Here is a link to the ICO website for further information on the fees: <https://ico.org.uk/media/for-organisations/documents/2258205/dp-fee-guide-for-controllers-20180221.pdf>

Should staff use their personal equipment (mobile phones, digital cameras etc.) to take photos or recordings of children?

We would strongly advise that the safest approach is to completely avoid the use of staff using any personal equipment or devices to take photos or recordings of children or to contact parents/carers, and to always use setting provided equipment or communication channels.

Use of personal devices can undermine the wider safeguarding culture within a setting. One potential danger of permitting staff to use personal devices to take photographs is that there could be an allegation following a misinterpreted or misunderstood approach; with a personal device it would be more difficult to prove that this was not the case. Any use of personal equipment to take or share images should be avoided, even if members of staff believe that individual children cannot be identified.

When using officially provided equipment and communication channels, protection is significantly increased for both children and staff. Many educational settings provide staff with a shared work camera/mobile phone, dedicated memory card and a separate, specific and approved email addresses or phone numbers to use.

Educational settings will need to put policies and procedures in place to avoid misuse of a work mobile phone e.g. password protected, only used by staff for work purposes.

Should educational settings decide to allow personal devices to be used by staff, such in emergency circumstances, this practice should be formally discussed with and recorded by the DPO and the Designated Safeguarding Lead (DSL). Leaders and managers should ensure there are clear and documented boundaries and procedures in place to ensure data protection legislation is followed, and that children and staff are appropriately safeguarded from harm or potential allegations. The decision by the educational settings management regarding this approach should be clearly and formally risk assessed, documented within appropriate policies and explicitly monitored by the DSL.

Can parents take their own photos or recordings at events?

Parents/carers taking pictures or recordings of their own children for their own personal use is lawful and should be allowed. The difficulty arises with events such as plays etc. in that other children may also be filmed. Parents must also be made aware that it is illegal to sell or distribute any such recording without proper permission.

When hosting an event where parents are permitted to take photographs or film footage, it is advised that settings make it clear from the start that any images taken must be for private use only. Educational settings might want to provide written guidance (see the appendix for samples) to parents beforehand and/or make an announcement at the start of the event.

A difficulty can arise when parents/carers attend official events in a voluntary or supportive capacity, such as parent volunteers on trips. In these situations, it is important that parents are aware that they are acting as members of staff and, as such, must abide by the settings policies and procedures. Parent volunteers should be informed about the image policy and expectations regarding their use

of personal devices. It is recommended that this is covered within a volunteer Acceptable Use Policy (AUP); this should be shared along with the expectations regarding confidentiality and safeguarding etc. with any volunteers before attending or supporting events.

Can parents or staff volunteer to take photos on behalf of the setting using their own equipment?

Many settings find that they have members of the community with access to high quality photography equipment, as well as novice and expert photography and videography skills. If settings choose to use parents, staff or indeed pupils in a voluntary capacity to take official photograph or videos, leaders will need to address the potential safeguarding and data protection/GDPR issues that can occur.

Can't educational settings just ban mobile phones and personal devices?

A policy which seeks to completely prohibit children, parents and staff from having or using mobile phones and cameras is likely to be viewed as unreasonable and unrealistic and complete bans can lead to a culture of suspicion, uncertainty and secrecy. Many staff and visitors would also be concerned for health and safety reasons if they were not allowed to carry a personal mobile phone as they may be used to stay in touch with family members.

DSLs, DPOs, leaders and managers should take appropriate steps to ensure that all members of staff understand the clear boundaries regarding professional use to protect children from harm and also themselves from allegations.

Derbyshire County Council's e-safety content can be found at:
<https://www.derbyshire.gov.uk/leisure/libraries/services/children-young-people/parents-carers/esafety/e-safety.aspx>

You can also find Safeguarding Children advice at:
www.getsafeonline.org/safeguarding-children

Can educational settings share images with parents/carers?

Educational settings will need to consider the safest, as well as most effective, way of sharing images with parents/carers. It is recommended that this decision is underpinned with a risk assessment approach to consider benefits and possible hazards for the range of channels being considered. If using email or text systems to share images, only setting provided devices, emails or phones should be used by staff and clear boundaries for use should be documented within the appropriate policies.

Use of staff personal devices or personal communication channels must not be used for official business or for sharing images with parents; this can bring both data protection and safeguarding risks for all members of the community.

In recent years there has been an increase in a range of applications (apps) for mobile devices have been launched which are targeted specifically at educational settings which allow staff to track and share a child's learning journey online with parents and carers, usually in the form of photographs and text. If settings are considering using such apps, leaders and managers must have a clear understanding of where and how children's data will be stored within the app/tool/system, including who has access to it and any safeguarding and data protection implications. Parents/carers and staff who have access to the app must be provided with clear boundaries regarding safe and appropriate use prior to accessing the service/system.

Schools and settings must be aware that leaders and managers are ultimately responsible for the security of any data or images held of children.

Educational settings need to be aware that once images have been shared with parents/carers, they are unable to control how the images are distributed, amended or altered. In most cases this is unlikely to be a concern, however if images contain other children, settings would need to ensure that all members of the community are aware of the expectations for safe use. For example, not sharing them on social media sites. Some settings request parents sign a disclaimer, agreement or acceptable use policy which highlights safe and responsible use of official school provided images before content is shared.

DPOs, head teachers, managers or leaders should carry out a Data Protection Privacy Impact Assessment (DPIA). A DPIA is a process which helps an organisation to identify and reduce the privacy risks of a project. An effective DPIA will be used throughout the development and implementation of a project, using existing project management processes. A DPIA enables an organisation to systematically and thoroughly analyse how a project or system will affect the privacy of the individuals involved.

The ICO has published information on PIAs here:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

Can images of children be taken off site by members of staff?

All images taken for official use should remain on site, unless prior explicit consent has been given by the DPO and the parent/carer of any child or young person captured in any photograph. When taking a memory stick or storage device containing images of children to be developed offsite, it should be suitably encrypted, logged in and out by the DSL or DPO and monitored carefully to ensure it is returned within the expected time scale. This would

include taking images off site on a CD or memory stick for report writing or printing purposes. This may also apply to many “apps” on smartphone’s or tablets.

Care must be taken that photographs are stored appropriately. For instance, if staff copy photographs on to a personal laptop as opposed to a setting allocated laptop or using an “app” it will be difficult to retain control of how the picture is use; this could lead to a breach of the Data Protection Act. Work provided, secure memory cards, secure remote access systems, memory sticks and CD’s should only provide a temporary storage medium and photographs should be uploaded to an appropriate area of the setting’s network as soon as possible and then erased immediately from their initial storage location.

If you send photographs of an event to the press, for example following a nativity play or sports day, settings must be aware that there is a risk they may fall into the wrong hands if transferred electronically. Email is not secure; settings should therefore take steps to suitably protect images, for example images being password protected.

Many settings upload images to third party websites for printing purposes; digital printing can often be cheaper and offer more security than taking images off site on a CD or memory stick. If settings wish to do so, they should use known and reputable sites and ensure the website or service being used has appropriate security measures in place by reading the websites terms and conditions and privacy policy.

Educational settings may wish to include this information on the image consent form so that parents/carers are aware that children’s images are going to be uploaded to a third-party website for printing purposes.

Educational settings need to be aware that when content (including images and videos) is uploaded to a third-party website, the user agrees to their terms and conditions; for some sites this could mean they have a license to copy, modify and use the images. This means the setting no longer “owns” the photo and it could be used externally for promotion and publicity purposes etc. without the setting’s consent or knowledge. Educational settings should ensure they read the terms and conditions and privacy policy of any websites they are using to identify if this is a risk. Educational settings may need to modify their image consent form accordingly to cover third party hosting. It is recommended that any images are suitably protected so that they could not be used without the settings’, and parents’, consent and knowledge.

Educational settings need to establish if it is possible to use the site in the first place, as some image hosting sites are only free for personal use. Professional or corporate use for some free services may be prohibited. This would mean that official use would breach the site terms and conditions.

Educational settings should undertake a DPIA (risk assessment) on any websites or apps etc. that may be used to share, host or access images to identify possible dangers and what actions may be required to limit any concerns. This would enable the DPO, leadership or management team to identify what action will be taken to safeguard children and staff, to ensure that the use of images (such as where the data will be hosted) complies with Data Protection legislation and the data security policy. Educational settings will also need to update staff training to ensure that all members of staff understand how to use the site/app safely and in accordance with both the law and settings policy.

How can managers, leaders, DPOs and DSLs enforce the policy regarding the use of personal phones and devices?

Managers, leaders, DPOs and DSLs should explore the benefits and risks of mobile phones and personal devices to ensure that a proportional and realistic policy decision is made. Where possible parents, children and staff should be included within this process to increase engagement and develop whole setting ownership of the policy.

Many settings also chose to display appropriate signage for visitors and volunteers or implement separate acceptable use policies (see the appendix for samples). Educational settings should implement an appropriate acceptable use policy (AUP) which clearly states expectations for safe use as well as any sanctions.

This should be supported with up-to-date, regular and robust whole staff training as part of staff induction data protection and child protection training; this should be provided for all members of staff on a regular basis. Leaders should ensure that they role model acceptable and safe behaviour with devices and image use to ensure good practice is consistent. Staff need to understand the risks associated with using their own phones or communication channels and how this can place themselves, and children, at risk so that the policy is not just seen as an arbitrary 'rule'.

Do we need written consent to take and use images of children?

Yes. The GDPR and Data Protection legislation affects the official use of photography by educational settings, as an image of a child is personal data. Therefore, written consent must be obtained from the parent of a child or young person under the age of 13 (or from the child him or herself if deemed to be competent to make such judgements from 13 years old) for any photographs or video recordings.

Verbal consent must not be accepted under any circumstance. If it is not possible to obtain prior written parental consent, then images must not be taken involving the individual child or young person concerned.

How long does consent last for?

As most children attend settings for a period of time (e.g. in Primary or Secondary schools, five years), it seems sensible to obtain consent for the whole period a child will be attending the setting, although settings can choose to request consent more frequently e.g. annually. Educational settings may wish to send a consent form to parents/carers with the registration pack, to cover the period that their children will spend at that setting.

Although this usually means that you won't have to renew parental or child consent until a child changes schools or transition stages (e.g. starts sixth form), you will have to be careful to record any changed circumstances. This will be easier if you keep photographs and signed consent forms together.

Educational settings also need consent from teachers and any other adults who may appear in the photograph etc., not just the children. A consent form for adults is available in the appendix.

You should not reuse photographs after a child (or member of staff) leaves the setting; it is recommended that settings destroy images immediately or obtain separate consent to continue to use the image for official purposes.

Do we need to obtain consent before taking photographs for educational setting administration purposes, e.g. for trips or management information system records?

If the images are not used for any other purpose, you will be acting lawfully in processing them. The problem arises when images are published or passed on to a third party without consent.

What if we publish a photograph without obtaining consent?

If you publish a photograph without consent then the parent (or child, if they have sufficient understanding) can make a complaint against the data controller to the Information Commissioner. In some cases this has resulted in fines for the organisation and damages being awarded to the person in the photograph.

Can we use existing images?

Educational settings may already have photographs or videos on file. If they are re-using older photographs where consent was obtained but only for paper publications, then it is recommended that you renew parental consent to use the images online.

If consent was never obtained, i.e. photos were taken before the legislation came into force, then settings should apply common sense when using them. For example, it would be unwise to use a picture of an untraceable person on a leaflet about a mental problem or an illness.

To help make a balanced decision when re-using photographs, it may be helpful to consider the following:

- For what purpose was the photograph originally taken, e.g. was it taken for a specific project such as your school/setting prospectus?
- Where was the photograph taken, e.g. was it taken in a public place?
- When was it taken, e.g. was it taken recently or a long time ago?

Although Data Protection does not relate to deceased people we would still give their personal data i.e. images in this instance the same amount of confidentiality.

If a parent, child or young person or member of staff supplies your school/setting with a photograph, then you should not automatically assume that they are giving their consent to subsequent publishing. Make sure you get a signed consent form before publishing in any official literature or online.

Can we put images of children or staff online, such as on our website or our official social media channels?

We recommend that educational settings websites and social media channels avoid using:

- Personal details or full names (first name and surname) of any child or adult in a photograph.
- Personal contact information such as email, postal addresses, and telephone or fax numbers.

If educational settings use a photograph of an individual child, they should not include that child's first name in the accompanying text or photo caption. If a child is fully named in the text, then it is recommended that settings don't include a photograph of that child. The same advice would apply to images of staff and the relevant consent should be obtained. This will reduce the risk of inappropriate and unwelcome attention from people outside the setting.

As an alternative, settings could ask children to draw a picture of a child or member of staff for the website. Additionally, settings could consider using group photographs with general labels such as "a science lesson" or "making Christmas decorations". Educational settings must remember that they must always get explicit consent, which means getting a signature, before publishing a photograph, of a child or adult, on the internet.

What about copyright?

Educational settings will need to be aware of copyright implications with any photographs that they might use from elsewhere e.g. online.

What about Webcams and CCTV?

The regulations for using webcams and CCTV (closed-circuit television) state that the area in which you are using the webcam/CCTV must be well signposted and people must know that the webcam/CCTV is there before they enter that area. In effect, this means you are getting their consent. This includes using webcams or other recording or streaming devices as CCTV.

As with photographs, you must tell the person:

- Why the webcam/CCTV is there
- What you will use the images for, and
- Who might want to look at the pictures

Further advice from the ICO regarding CCTV can be accessed at: <https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/>

What if something goes wrong?

The Information Commissioner's Office has the power to impose huge fines (up to £17 million) on Data Controllers for breaching the GDPR and the Data Protection Act.

The legislation states that

“Personal information must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures”

There are several tools that the ICO can use to act to change the behaviour of organisations and individuals that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement, audit and a monetary penalty notice. The ICO can also issue undertakings committing an organisation to a course of action to improve its compliance.

Here are a few examples of undertakings that have been signed in the past by schools:

1. A complaint about the way in which a Nursery School had been dealing with the personal data they hold has been investigated by the Information Commissioners Office and subsequently the nursery has been found in breach of the legislation. They have signed an undertaking to ensure they will improve procedures for handling personal information and to ensure that members of staff are trained on how to follow them. In this instance the nursery lost a backup tape containing the personal details of 70 pupils and their parents or guardians (there was also some health-related information held on the back up).
2. An undertaking to comply with the seventh data protection principle has been signed by a School. This follows the theft of an unencrypted laptop containing personal data relating to nine pupils. The data controller was subject to a burglary on its premises during which the

laptop was stolen. The laptop was stored in a locked filing cabinet but the office itself was not locked.

3. An undertaking to comply with the seventh data protection principle has been signed by a School after the personal details of nearly 20,000 individuals, including some 7,600 pupils, were put at risk during a hacking attack on its website.
4. An undertaking to comply with the seventh data protection principle has been signed by a Community Playgroup. This follows the theft of an unencrypted laptop containing personal information relating to approximately 47 families.

There is a duty to report certain types of personal data breaches to the ICO within 72 hours, where there is a risk of affecting an individual's rights and freedoms.

Below are links to the ICO guidance on data protection breaches

- <https://ico.org.uk/for-organisations/report-a-breach/>
- <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

What should I do if I am concerned about current practice in my setting?

If educational settings are unsure of their legal responsibilities in relation to the use of images, they can consult with the relevant person from the Local Authority – see contacts page for information.

Any evidence of the use of inappropriate images, or the misuse of images by any member of the community should be reported to the educational setting's Data Protection Officer (DPO) and designated safeguarding lead (DSL) who may then consult with Derbyshire County Council Children's Services or the police, if appropriate.

Supporting Advice and Guidance

The following information has been provided to ensure that educational settings are able to make appropriate and informed decisions in relation to the use of images and videos.

Legislation and Consent

The GDPR and Data Protection legislation impacts on the official use of photography by all educational settings. This is because an image of a child is personal data and it is a requirement that written consent is obtained from the parent of a child or young person under the age of 13 (or from the child him or herself if deemed to be competent to make such judgements from 13 years old) for any photographs or video recordings. It is also important for settings to

ascertain the views of the child regarding their images at any age. Some settings ask permission to publish images of work or appropriate personal photographs on admission to the setting, some once a year, others at the time of use.

In some circumstances it might be difficult to obtain parental consent. For example, settings should exercise caution when dealing with looked after children; it may be appropriate to get consent from the carer, as well as the child or young person.

Verbal consent must not be accepted under any circumstance. If it is not possible to obtain prior written parental consent, then images must not be taken involving the individual child or young person concerned.

The parent or carer has the right to refuse or withdraw their consent at any time. Partial or restricted consent can also be given where deemed necessary by the parent or carer.

Images of children who no longer attend the setting must not be used, unless specific consent has been obtained to cover this extended period. Generally, consent to use images lapses when a child leaves the setting.

Images of children for which consent has never been given are not to be used, unless the specific consent of the parent or carer is obtained. Should it not be possible to obtain such consent, then images must be returned to the individual concerned or destroyed.

If two parents disagree over consent for their child to appear in photographs or in DVD recordings, then settings should have to treat it as if consent has not been given. Likewise, if the parents give their consent but the child does not, then it is safer to assume that consent has not been given.

Planning Photographs of Children and Young People

Still and moving images and sound add liveliness and interest to a publication, particularly when children can be included, nevertheless, the security of staff and children is paramount. Published images could be re-used, particularly if large images of individual children are shown. Although common in newspapers, the publishing of children's' names with their images is not acceptable.

Strategies include using general shots e.g. classrooms and group activities which would include relatively small images of groups of children. "Over the shoulder" can replace "passport style" photographs but still convey the activity. Personal photographs can be replaced with self-portraits or images of children's work or of a team activity. Children in photographs should, of course, be appropriately clothed and written consent should be obtained for all children in the picture.

There will also be times where organisations will be carrying out off-site activities e.g. activity holidays or educational visits. In these circumstances it is likely that the organisation will want to make some visual record. It is also likely that children and young people will want to make their own visual records, so it is important that organisations develop policies and guidelines on the use of mobile phone with cameras and digital cameras.

Settings should recognise that some children, young people and adults will be more vulnerable than others, for example disabled children, children in care, those with a child protection or child in need plan, those with English as an additional language, black, minority and ethnic children and those who have been subject to domestic abuse. For a range of reasons, such children's (and indeed adults) security may be compromised more than others, and therefore extra precautions must be considered in such circumstances.

The taking of images of a child or young person in a one to one situation with an adult is to be avoided whenever possible; unless there is an agreed, specified reason for doing so. It must be recognised that the context of such situations is likely to be perceived as sensitive and the use of cameras can be intrusive and open to misinterpretation. It should be recognised that this may leave both the adult and child in a vulnerable position and is therefore not considered as accepted practice.

Settings must always ensure that they use images of children in suitable dress and take care photographing PE or swimming events to maintain modesty, using team tracksuits if appropriate for example. Settings should be aware that children could be identified by logos or emblems on sweatshirts etc.

Settings should also remember to include images of children from different ethnic backgrounds in your communications wherever possible, and positive images of children with disabilities to promote your settings as an inclusive community, and to comply with the Disability Discrimination Act.

Identifying Children and Young People in Images Online

The advice and guidance from DCC with regards to identifying children and young people is as follows:

- If the child is named with first name and surname, settings should avoid using their photograph
- If a child in a photograph is to be named, the setting should avoid fully naming the pupil

We would also recommend that settings use the minimum information and consider whether it is necessary to accompany a picture with personal information e.g. children's names, the year group, and the setting name.

If a setting wishes to fully name children in any published text, whether in a brochure, website, social media channel or in the local press, it is recommended they avoid using a photograph unless they have specific written parental consent to do so.

Use of Photos/Videos by Parents/Carers

Under GDPR and Data Protection legislation any photos taken for official setting use may be covered by the legislation and parents/carers and children should be advised why they are being taken. Any photos taken purely for personal use (such as by parents at events to put into a family album) are exempt from the legislation.

Where parents are permitted to take photographs or DVD footage, settings should make it clear from the start that any images taken must be for private use only. Settings might want to provide written guidance to parents beforehand (e.g. as part of information given to parents when new children join the setting) and/or make an announcement at the start of each event. Parents are not permitted to take photographs or to make a video recording for anything other than their own personal use.

The right to refuse parents and carers the opportunity to take photographs and make videos is, however, to be reserved on health and safety grounds. For example, if an excessive use of flashlights and/or bulky and noisy equipment are to be considered a potential health and safety risk.

Settings should ensure that individuals with no connection to the setting are not given any opportunity to film covertly. Members of staff have the authority to question anybody they do not recognise (while maintaining their own safety) should they be observed using any photographic equipment at events and productions or within the general vicinity.

Use of Photos/Videos by Children and Young People

Many settings have digital cameras/videos which are used by the children to document their activities and as part of learning. This is a useful tool to support children's education. However, the use of digital cameras by children should always be appropriately supervised by staff to ensure that images are taken in a safe and enabling environment.

It is possible that if children are left unsupervised with a camera that they could unintentionally or intentionally take inappropriate or even illegal images of themselves or other children (such as images which may show children in a state of undress). This could potentially lead to criminal offences occurring and could place children and staff at risk, for example if the images are taken off site by a member of staff or accidentally shared online or on a digital screen with parents or visitors. This behaviour could also normalise unsafe activity for children which could be taken advantage of by people who abuse children.

If children are taking images for official use by the setting, rather than for personal use, they will be covered under GDPR and the Data Protection Act, meaning consent will be required.

Staff should discuss and agree age appropriate acceptable use rules for cameras etc. with children, such as places children cannot take the camera (e.g. unsupervised areas, toilets etc.). Staff should be fully aware of the acceptable use rules and ensure that children are appropriately supervised when they are using cameras. Staff should role model positive behaviour to the children by encouraging them to ask permission before they take any photos. Photos should be carefully controlled and checked before sharing with parents/carers online or via digital screens. Still or video cameras provided for use by children and the images themselves must not be removed from the setting.

Parents should be made aware that children will be taking photos/videos of other children and should be informed how these images will be managed by the setting e.g. will be for internal use by the setting only (not shared online or via any website or social media tool). This is extremely important to safeguard vulnerable children (e.g. adopted children or children in care). If parents/carers do not give consent for their children's images to be taken in this way, the setting must ensure those wishes are followed and that images are not taken.

Educational settings will have policies on use of personal devices by children and young people. Where such equipment is allowed, it is important that all settings have Acceptable Use Policies (AUPs) which cover safe usage and possible consequences of misuse e.g. areas of increased concern would involve residential trips and usage in bedrooms or swimming. Children and young people need to be made aware that taking and distributing illegal photographs may be a criminal offence and inappropriate use of photography will result in disciplinary action.

Storage of Images and Videos

Should images need to be kept for a short period of time, they must be protectively stored. This may include password protection and encryption.

- Images should never be stored on personal devices
- Equipment which contains images must always be stored securely and access should be restricted
- Photographs should only be stored on portable storage devices for a temporary period; explicit permission must be obtained from the DPO and/or DSL and effective security measures must be in place

Any use of social media, tracking apps or cloud storage to store or share images and videos must be appropriately risk assessed and the DPO, leader/managers

must ensure appropriate written consent is obtained and that the educational setting have responsibility for the uploading and distribution.

Images must always be stored and disposed of securely to prevent unauthorised access, ensure confidentiality and protect identity. All images must to be stored and disposed of in line with GDPR and the Data Protection Act.

Use of Images of Children by the Media

There may be occasions where the press are invited to a planned event to take photographs of the children and young people who take part. It should be noted that the press has special rights under the Data Protection Act, which permit them to publish material for journalistic purposes.

Generally, parents and carers will take pride in 'press cuttings'. For the majority, this pride will often outweigh any fears about the image and/or information being subject to misuse. However, some parents may object to information about, and images of, their own children being published. As a result, parental/carers consent must be sought before the press is given any access to children and young people. Should a parent or carer choose not to give permission for their child to be photographed in such circumstances, this right must be observed at all times.

The way the press will use images is to be controlled through relevant industry codes of practice as well as the law. In this way a check is to be put on the potential improper use of images of children and young people by the press.

Additional checks should also be carried out by the DPO and/or the DSL to ensure that broadcasters and press photographers are made aware of the sensitivity which must be considered in respect of detailed captioning, one to one interviews, and close sports photography.

Use of External Photographers/Videographers

Any external photographers (including staff or parent volunteers) who are engaged to record or photograph any events on behalf of the setting (such as at school events) must be prepared to work according to the terms of the settings policy as well as the following guidelines:

- In the context of data protection legislation, the photographer will be considered a 'data processor' and any agreement with them will be in accordance with the GDPR and Data Protection legislation
- Photographers will only be used where they will guarantee to act appropriately to prevent unauthorised or unlawful processing of images; and will insure against accidental loss or destruction of, or damage to, personal data

Photographers should be asked to sign an agreement with the settings which will aim to ensure:

- Compliance with GDPR and other Data Protection legislation
- Awareness of their specific responsibilities and accountability in line with GDPR and Data Protection legislation
- That images:
 - Are only to be used for a specified purpose and will not be used in any other context
 - Are kept securely in accordance with GDPR and data protection legislation
 - Will only be kept for an agreed length of time and will be disposed of in line with GDPR and data protection legislation
 - Will not be disclosed to any third party unless it is a specific requirement in order to fulfil the requirements of the agreement. Such use will also be subject to parental/carers permission

Details of any checks regarding suitability, which would include awareness of GDPR and Data Protection legislation as well as evidence of appropriate checks e.g. DBS (Disclosure and Barring Service) must be requested.

Photographic identity of photographers should be checked on arrival. Should there be any concerns in respect of the authenticity of any photographer, then entry should be refused and reported, as is deemed appropriate.

It is recommended that reputable photography agencies and/or professional photographers are used by the setting. Educational settings which allow volunteers (e.g. parents or staff) to formally video or photograph productions or events on behalf of the school (such as to create a video or DVD for parents and children) will need to consider if this approach can be managed in accordance with GDPR and data protection legislation. Some settings have required volunteers to only use setting provided equipment and systems to take and edit videos and have used encrypted USB drives or systems to ensure data is transfer and held in accordance with the data protection act.

Use of Closed-Circuit Television (CCTV)

Any settings use of CCTV should be developed in accordance with the CCTV Code of Practice from the Information Commissioner's Office. The Code of Practice was updated in 2017 and provides guidance and advice for CCTV users on how to comply with Data Protection legislation and also includes a simple checklist for users of very limited CCTV systems where the full provisions of the code would be too detailed: <https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

CCTV may be used for the following purposes:

- To control access
- To monitor security

- For site management, for example monitoring incorrect parking, manoeuvring vehicles and delivery arrivals
- For monitoring purposes, particularly within the building, in corridors and areas out of sight or not frequently trafficked by staff, for example in the vicinity of toilets (but not in toilet cubicles)
- For general and focused observations of children, young people and staff
- To act as an effective deterrent to prevent crime and to discourage trespass

When settings decide to use CCTV or are reviewing its continued use, they should take into account the benefits of using surveillance cameras. They must also consider whether better solutions exist, as well as the effect it may have on individuals within, and an assessment should take place to determine whether CCTV is justified and its impact. It is extremely important that settings seek the views of all those who are subject to surveillance, staff, children and their families, and respond to these views accordingly.

Settings should regularly review whether the use of surveillance systems continues to be justified. It might be helpful to carry out a Data Privacy Impact Assessment (DPIA).

All areas which are covered by CCTV must be well signposted, and notifications must be displayed so that individuals are advised before entering such vicinity. The objective for the use of CCTV should be justified and communicated appropriately with the community e.g. if it is used for security or safeguarding purposes.

The use of CCTV by settings must ensure that the manufacturer's instructions and data protection and information sharing guidelines are always followed. This should include the appropriate storage and disposal of all recordings.

Every effort must be made to avoid inadvertently taking inappropriate images and therefore cameras must be placed and positioned sensitively. No cameras should be pointed directly at toilet cubicles or any other sensitive areas within the setting environment.

Use of Webcams

Some settings are now using webcams as an alternative to CCTV. Regardless of whether webcams are being used as a security/safety tool or for an educational purpose, it is recommended that consultation should be carried out with children, young people, parents and carers, practitioners and their managers to determine if they agree to being filmed.

As with static images, written consent must be obtained from all parents and carers. Before seeking such consent, full details of why a webcam is to be used should be provided. This should include information on the use of images, who

is to be given authority to view them, and the security measures which will be implemented to prevent unauthorised access.

If settings are using webcams for safety or security purposes, the regulations which apply to webcams regarding signage will be the same as for the use of CCTV.

Copyright

It is important to be sure of the copyright position of any photographs schools/settings intend to use, because photographic images are considered as artistic works under the laws of copyright.

Copyright is the right given to authors and creators of works, such as books, films or computer programs, to control the exploitation of their works. This right broadly covers copying, adapting, issuing copies to the public, performing in public and broadcasting the material. Copyright arises automatically and does not depend on the completion of any formalities, such as registration.

Educational settings should be aware that photographs obtained from the internet are also subject to copyright. The first owner of copyright is usually the author of the work. The major exception is where such work is made in the course of employment, in which case the employer owns the copyright.

Commissioning and paying for work does not procure the copyright. Contractors and freelancers own the first copyright in their work unless the commissioning contract agrees otherwise.

Educational settings should also remember that copyright lasts for over 50 years. Photographs taken after 1 August 1989 are protected for 70 years after the death of the photographer. There are different rules regarding older photographers depending on the relevant Copyright Act at the time they were taken. See the table below.

Date Photograph Taken	Length of Copyright
Before 1912	Expired
1 st July 1912 to 1 st June 1957	50 years from the end of the year in which the photograph was taken
1 st June 1957 to 1 st August 1989	70 years from when the negative was taken
After 1 st August 1989	70 years after the death of the photographer

It is the settings responsibility to ensure that all photographs used on their website have this credit applied.

More information on copyright is available from:
United Kingdom's Copyright Licensing Agency: <http://www.cla.co.uk/>

International Federation of Reproduction Rights Organisation:
<http://www.ifrro.org/>

Aston on Trent Primary School Image Use Policy

Policy written by: S Moore (adapted from DCC model policy)

Approved by Governing Body on: November 13th 2023

Date to be reviewed: Annually

School/Setting Data Controller: Sam Moore

School/Setting Designated Safeguarding Lead (DSL): Sam Moore

Governor with lead responsibility: Clare Coles

Official use of Images/Videos of Children

Scope and aims of the policy

This policy seeks to ensure that images and videos taken within and by Aston on Trent Primary School are taken and held legally and the required thought is given to safeguarding all members of the community.

This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers.

This policy must be read in conjunction with other relevant school policies including, but not limited to; safeguarding and child protection, anti-bullying, behaviour, data security, image use, Acceptable Use Policies, confidentiality, screening, searching and confiscation and relevant curriculum policies including computing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE).

This policy applies to all images, including still and video content taken by Aston on Trent Primary School.

All images taken by Aston on Trent Primary School will be used in a manner respectful of the Data Protection Principles. This means that images will be processed:

- fairly, lawfully and in a transparent manner
- for specified, explicit and legitimate purposes
- in a way that is adequate, relevant limited to what is necessary
- to ensure it is accurate and up to date
- for no longer than is necessary
- in a manner that ensures appropriate security

The Data Protection Officer (DPO) within the setting, supported by the DSL and management team, are responsible for ensuring the acceptable, safe use and

storage of all camera technology and images within the setting. This includes the management, implementation, monitoring and review of the Image Use Policy.

Parental consent

Written permission from parents or carers will always be obtained before images and/or videos of children are taken, used or published.

Written parental consent will always be sought to take and use photographs offsite for professional, marketing and training purposes. This may be in addition to parental permission sought for onsite images.

Written consent from parents will be kept by the setting where children's images are used for publicity purposes, such as brochures or publications, until the image is no longer in use.

Parental permission will be sought on an agreed basis when a child enters Aston on Trent Primary School, and will remain valid for the duration of the child's time here.

A record of all consent details will be kept securely on file. Should permission be withdrawn by parents/carers at any time, then all relevant images will be removed and disposed of and the record will be updated accordingly.

Safety of images and videos

All images taken and processed by or on behalf of the school will take place using school approved equipment and devices.

Staff will receive information regarding the safe and appropriate use of images as part of their data protection and safeguarding training.

All members of staff, including volunteers, will ensure that all images are available for scrutiny and will be able to justify any images in their possession.

Images will not be kept for longer than is to be considered necessary. A designated member of staff (DPO or DSL) will ensure that all photographs are permanently wiped from memory cards, computer hard and portable drives or other relevant devices once the images will no longer be of use.

All images will remain on site, unless prior explicit consent has been given by both DPO and DSL and the parent or carer of any child or young person captured in any photograph. Should permission be given to take any images off site then all relevant details will to be recorded, for example who, what, when and why and data will be kept securely for example with appropriate protection. Any memory stick, CD or storage device containing images of children to be taken offsite for further work will be suitably protected and will be logged in and

out by the DPO and/or DSL; this will be monitored to ensure that it is returned within the expected time scale.

The DPO and/or DSL reserve the right to view any images taken and can withdraw or modify a member of staffs' authorisation to take or make images at any time.

Only official setting approved equipment and cameras will be used by staff to capture images of children for official purposes. Use of personal equipment and cameras by staff is prohibited, without authorisation from the head teacher.

Any apps, websites or third-party companies used to share, host or access children's images will be risk assessed prior to use.

The school will ensure that images always are held in accordance with the General Data Protection Regulations (GDPR) and Data Protection Act, and suitable child protection requirements, if necessary, are in place.

Photographs will be disposed of should they no longer be required. They will be returned to the parent or carer, deleted and wiped or shredded as appropriate. Copies will not be taken of any images without relevant authority and consent from the DPO and/or DSL and the parent/carer.

Publication and sharing of images and videos

Images or videos that include children will be selected carefully for use, for example only using images of children who are suitably dressed.

Images or videos that include children will not provide material which could be reused.

Children's' full names will not be used on the website or other publication, for example newsletters, social media channels, in association with photographs or videos.

The school will not include any personal addresses, emails, telephone numbers, fax numbers on video, on the website, in a prospectus or in other printed publications.

The school uses Parenthub to upload and share images of children with parents.

The use of the system has been appropriately risk assessed and the headteacher has taken steps to ensure all data stored is held in accordance with GDPR and the Data Protection Act.

Images uploaded to Parenthub will only be taken on school approved devices.

Parents/carers will be informed of the expectations regarding safe and appropriate use (e.g. not sharing passwords or copying and sharing images) prior to being given access. Failure to comply with this may result in access being removed.

Safe Practice when taking images and videos

Careful consideration is given before involving very young or vulnerable children when taking photos or recordings, who may be unable to question why or how activities are taking place.

The school will discuss the use of images with children and young people in an age appropriate way.

A child or young person's right not to be photographed is to be respected. Images will not be taken of any child or young person against their wishes.

Photography is not permitted in sensitive areas such as changing room, toilets, swimming areas etc.

Use of photos and videos of children by others

Use of photos and videos by parents/carers

Parents/carers are permitted to take photographs or video footage of events for private use only.

Parents/carers who are using photographic equipment must be mindful of others, including health and safety concerns, when making and taking images.

The opportunity for parents/carers to take photographs and make videos can be reserved by the school on health and safety grounds.

Parents/carers are only permitted to take or make recording within designated areas of the school. Photography is not permitted in sensitive areas such as changing room, toilets, swimming areas etc.

The right to withdraw consent will be maintained and any photography or filming on site will be open to scrutiny at any time.

Parents may contact the school DPO/DSL to discuss any concerns regarding the use of images.

Photos and videos taken by the school and shared with parents should not be shared elsewhere, for example posted onto social networking sites. To do so may breach intellectual property rights, data protection legislation and importantly may place members of the community at risk of harm.

Use of photos/videos by children

The school will discuss and agree age appropriate acceptable use rules with children regarding the appropriate use of cameras, such as places children cannot take the camera, for example unsupervised areas, toilets etc.

The use of personal devices e.g. mobile phones, tablets, children's own digital cameras, is covered within the schools mobile phone and/or online safety policy.

All staff will be made aware of the acceptable use rules regarding children's use of cameras and will ensure that children are appropriately supervised when taking images for official or curriculum use.

Members of staff will role model positive behaviour to the children by encouraging them to ask permission before they take any photos.

Photos taken by children for official use will only be taken with parental consent and will be processed in accordance with GDPR and the Data Protection Act.

Parents/carers will be made aware that children will be taking photos/videos of other children and will be informed how these images will be managed. For example, they will be for internal use by the setting only and will not be shared online or via any website or social media tool.

Photos taken by children for official use will be carefully controlled by the school and will be checked carefully before sharing online or via digital screens.

Still and video cameras provided for use by children and the images themselves will not be removed from the setting.

Use of images of children by the media

Where a press photographer is to be invited to celebrate an event, every effort will be made to ensure that the newspaper's, or other relevant media, requirements can be met.

A written agreement will be sought between parents and carers and the press which will request that a pre-agreed and accepted amount of personal information (such as first names only) will be published along with images and videos.

The identity of any press representative will be verified and access will only be permitted where the event is planned, and where press are to be specifically invited to attend. No authorisation will be given to unscheduled visits by the press under any circumstances.

Every effort will be made to ensure the press abide by any specific guidelines should they be requested. No responsibility or liability however can be claimed

for situations beyond reasonable control, and where the setting is to be considered to have acted in good faith.

Use of external photographers (this may include volunteers such as staff or parents)

External photographers who are engaged to record any events will be prepared to work according to the terms of the settings online safety policy.

Photographers will sign an agreement which ensures compliance with GDPR and the Data Protection Act.

Images taken by external photographers will only be used for a specific purpose, subject to parental consent.

Photographers will not have unsupervised access to children and young people

Children's Images: Frequently Asked Questions for Parents/Carers

Why do we need a policy?

Schools, playgroups, nurseries and youth groups have always used photographs as a way of celebrating achievement or seeking publicity for fundraising etc. Families and children often enjoy seeing their loved ones in print or on a website. We want to ensure that everyone can continue to enjoy these activities safely. However, parents/carers need to be aware that placing any identifying information in the public domain has risks and will need to understand these issues to give properly considered consent. It is important that parents/carers and educational settings can fully consider the issues before any problems can arise.

So, what are the risks?

The most highly publicised and worrying risk is that a child who appears in the paper or on a web site may become of interest to a predatory sex offender. Locating people through the internet has become extremely easy, using widely available software, so if there is a picture and the name of a school/setting together with the name of the child then it could be quite easy to find out the child's address and even work out their likely route to school/setting. There are also other specific groups of children and families whose safety could be put at risk if identified e.g. families fleeing domestic abuse. To limit these potential risks, we will take appropriate steps, as outlined in the attached consent form, to safeguard children and the wider community.

Isn't this just scaremongering?

Sadly not. There have been cases of families receiving unwelcome phone calls following appearances in the press. However, this is rare, so it is important to have a sense of proportion in these matters. Remember we want to celebrate success and achievement but parents must be aware of risks to make an informed decision.

What about school/setting websites?

The same concerns apply to school/setting controlled online sites; there is an added concern that images of children can be copied, manipulated or changed by another person. We can try to copy protect images and will use lower quality images, but this can be bypassed so cannot not be relied upon to keep images safe.

I want to do my own recording of the school/setting play/event is this okay?

Taking pictures or recordings of your own children for your own personal use is okay. The difficulty arises when other children are also be filmed. It is important that we are all aware that some members of the community may be vulnerable and must not have their image shared online as they could be put at risk from harm. You may not always know who these people and we need everyone's support to protect the whole community. It's also important for us all to role model positive behaviour for children, so it might be a sensible idea to check first before posting any images online which contain other children than your own.

Parents/carers should not copy images from the school website without appropriate permission from the school.

Acknowledgement

This template policy is based on a document originally created by Kent County Council