

# Frittenden Church of England Primary School

## Image Use in an Educational Setting Policy



**Learning for Life in the Light of God.**

<b>Policy Control</b>	
<b>Responsible Person:</b>	<b>Nichola Costello</b>
<b>Responsible Governor Team:</b>	<b>Circle Model</b>
<b>Approved by Governors:</b>	<b>27<sup>th</sup> March 2018</b>
<b>Date due for review:</b>	<b>March 2020</b>

***Our school policies are written with the objective of continuously improving the school in our aim of realising the school's vision:***

### **Our Vision**

To engage every child in an exciting and meaningful educational experience, in an inclusive caring Christian Community

### **Our School Values**

Frittenden Church of England Primary School values

**Compassion • Wisdom • Hope • Trust • Thankfulness • Forgiveness**

and all our stakeholders are encouraged to *reflect* upon their learning and their actions.

# Contents

Introduction  
Frequently Asked Questions for Schools/Settings  
Supporting Guidance and Information  
Image Use Policy  
Template letters and other supporting documents  
Useful Contacts

This document is provided as guidance and as a possible template for schools and settings to use and adapt in order to establish safe practice when taking photos and videos of children and young people. These documents will need to be adapted according to individual schools/settings requirements and carefully consideration will be required by Managers (Senior Leadership Teams, Governing Bodies etc.) when considering how to implement safe practice across the whole school/setting community.

Kent Schools and settings can contact the Education Safeguarding Adviser (Online Protection) to discuss safe practice: [esafetyofficer@kent.gov.uk](mailto:esafetyofficer@kent.gov.uk) and further information regarding online Safety can be found at [www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety](http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety)

## Disclaimer

**Kent County Council (KCC) makes every effort to ensure that the information in this document is accurate and up to date. If errors are brought to our attention, we will correct them as soon as practicable. Nevertheless, KCC and its employees cannot accept responsibility for any loss, damage or inconvenience caused as a result of reliance on any content in this publication**

# Introduction

This use of images policy applies to the use of any film and electronic photographic equipment. This will include 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 digital cameras and mobile phones have become more advanced and easier to use, it is increasingly likely that children and their families will be using digital photography as part of their family life. It is therefore very important that all education settings consider the impact such technology may have.

Digital technology has increased the potential for cameras and images to be misused and inevitably there will be concerns about the risks to which children and young people may be exposed. However settings must be aware that the behaviours of individuals using the technology present the risk, not the technology. .

This document has been developed after discussions between Kent County Council, the press, early year's settings, schools and safeguarding staff. In developing such a policy for your own school/setting we suggest that head teachers, governing bodies and other managers 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.

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 by a stranger is small. By taking reasonable steps to make certain that a photograph is appropriate and the full name and contact details are protected, then photography for setting and other events by staff, families and the media should be allowed. We are aware that the widespread use of mobile telephones as digital cameras would make banning them very difficult for settings to impose and police. Generally photographs for school/setting and family use and those that appear in the press are a source of pleasure and pride. They enhance self-esteem for children and young people and their families and this practice should continue within safe practice guidelines.

Under the EYFS (3.4 "The safeguarding policy and procedures must ... cover the use of mobile phones and cameras in the setting") all settings and foundation stage providers must have a policy which covers the use of mobile phones and cameras within the setting. It is advisable that this policy covers the range of devices available, such as tablets, phones etc. Managers and Designated Safeguarding Leads (DSLs) must ensure that the settings policy covers specific expectations for safe and responsible use for mobile phones and personal devices by children, staff and others.

The school/setting will need to amend and adapt the sample materials included in this document according to the school/setting ethos and the technology used. The setting's Image Policy should ensure that it applies to and is understood by all individuals who are to have access to and/or be 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 DSL and/or the Management 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 and /or DSL can reserve the right to view any images taken and/or to withdraw or modify a member of staffs' authorisation to take or make official images at any time. All members of staff and their managers must ensure that all images are available for scrutiny and be able to justify any images in their possession. Settings can contact their Area Safeguarding Adviser or the Education Safeguarding Adviser (Online Protection) from the Education Safeguarding Team if they wish to discuss their current practise.

This guidance 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 have used 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 but 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 Schools and 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 derive great pleasure from 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 in order to give properly considered consent. It is also important that parents and settings have the opportunity to fully consider the issues before any problems arise.

## 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. Schools and settings may not always be aware of who these vulnerable groups may be.

## Isn't this just scaremongering?

Sadly not. We have had cases in Kent of families and staff receiving unwelcome phone calls or visits following appearances in the press or on school/setting websites. 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/carers must be aware of risks in order to make an informed decision.

Whilst ultimate responsibility for abuse lies with perpetrators, a staff culture which is complacent (e.g. "it couldn't happen here"), unclear and therefore or unsafe can facilitate an environment whereby abuse is not recognised which in turn places children at significant risk of harm. Clear and understood boundaries regarding safe and appropriate use ensures that all members of staff are able to identify and challenge poor practice. A culture with clear expectations for safe and responsible use of personal devices which is enforced by an informed and aware management is essential.

## Does the Government have a policy for schools/settings on the use of photographs?

No. The following was posted on the DfE Website (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](http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx)

Kent County Council's Access to Information Content can be found at <http://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information>

## Do we have to register with the ICO?

Data Controllers are people or organisations who hold and use 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 Data Protection Act 1998, in particular the 8 data protection principles of good information handling.

If you store personal data on a computer then you must register with the Information Commissioner's Office (the independent body that monitors the legislation), this is known as 'notification'. Failure to notify is a criminal offence.

Data controllers who are exempt from notification must comply with the other provisions of the Act, and may choose to notify voluntarily.

Here is a link to the ICO website for further information on notification:

[http://www.ico.gov.uk/for\\_organisations/data\\_protection/notification.aspx](http://www.ico.gov.uk/for_organisations/data_protection/notification.aspx)

There is a self-assessment tool which will explain whether or not there is a requirement for you to notify.

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

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

One potential danger of permitting members of staff to use personal devices or communication is that there could be an allegation following a misinterpreted or misunderstood message or approach and with a personal device/communication it would be more difficult to prove that this was not the case. Use of personal devices can also potentially undermine the wider safeguarding culture within a setting.

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

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. However if personal devices are used in emergency circumstances then this practice should be discussed with and approved by the settings Designated Safeguarding Lead (DSL), and there must be clear 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 school/setting's 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 photos/recordings at school/setting 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 DVD footage, it is advised that settings make it clear from the start that any images taken must be for private use only. Schools/Settings might want to provide written guidance to parents beforehand and/or make an announcement at the start of the event. (See the appendix for samples)

A difficulty can arise when parents/carers attend official events in a voluntary or supportive capacity, such as parent helpers/volunteers on school trips. In these situations it is important that parents are aware that they are acting as members of staff for the purpose of the trip and as such must abide by the school/settings policies and procedures. Parent volunteers should be informed about the school/settings image policy and expectations regarding their use of personal devices etc. It is recommended that this is covered within a volunteer Acceptable Use policy (template AUPs for schools and settings to adapt are available at [www.e-safety.org.uk](http://www.e-safety.org.uk)) and is shared with parents, along with the expectations regarding confidentiality and safeguarding etc. with any volunteers before attending or supporting events.

## Can't we just ban mobile phones and personal devices?

A policy which seeks to completely prohibit children, parents and staff from having/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, leaders and managers should take appropriate steps to ensure that all members of staff understand the clear boundaries regarding professional use so as to protect children from harm and also themselves from allegations.

The Kent County Council Online Safety policy template contains further information regarding mobile phones and personal devices: <http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety>

## Can schools/settings share images with parents/carers?

Schools and settings will need to consider the safest as well as more effective way of sharing images with parents/carers when considering systems such as email, text or applications. It is recommended that this approach 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 with parents/carers then only setting provided devices, emails or phones should be used 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 school/setting business or sharing images with parents as this can be both a data protection and also a safeguarding risk 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 education 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 purchasing or accessing any apps for staff or children's use, 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.

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

It also might be helpful in some cases for headteachers, managers or leaders to carry out a Privacy Impact Assessment (PIA). A PIA is a process which helps an organisation to identify and reduce the privacy risks of a project. An effective PIA will be used throughout the development and implementation of a project, using existing project management processes. A PIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved. The ICO website has a Code of Practice on PIAs: <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>

## Can images of children be taken off site by members of staff e.g. for report writing at home, online image/video hosting or for printing purposes?

All images taken for official use should remain on site, unless prior explicit consent has been given by the Data Controller 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 Data Controller 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 printing purposes and settings should also note that this would apply to many “apps” which might be used on Smartphone’s or tablets.

Care must be taken that photographs are stored appropriately. For instance to copy the photograph on to a personal laptop as opposed to a setting allocated laptop or using an “app” might make it difficult to retain control of how the picture is used and could lead to a breach of the Data Protection Act. Work provided, secure memory cards, 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 a school/setting event to the press, e.g. a nativity play or sports day, then settings must be aware that there is a risk that they may fall into the wrong hands if transferred electronically. Email is not secure so schools/settings must take steps to suitably protect images i.e. staff should password protect images before taking them off site.

Many schools/settings choose to upload images to third party websites for printing purposes as digital printing can often be cheaper and offer more security than taking images off site on a CD or memory stick. If schools/settings wish to do so, then they should ensure the website or service being used is appropriate by reading the websites terms and conditions. It is also recommended that settings use known and reputable sites. Schools and settings may wish to include this information on the 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.

Schools and settings must be aware that when content including images or videos is uploaded to a third party website then the user agrees to their terms and conditions and for some sites this would mean that by uploading any images schools/settings are granting the site a license to copy, modify and use the images. This means the school/setting no longer "owns" the photo which could mean it could be used externally by the website (or other users) for promotion, publicity purposes etc. without the school/setting’s consent or knowledge. Schools and settings need to fully read the terms and conditions and privacy policy of any websites they are considering using to identify if this is a risk. Schools and settings would need to modify their image consent form for parents accordingly to cover third party hosting. It is recommended that any images are suitably protected so that they could not be used without the school/setting’s (and parents) consent and knowledge.

Schools and settings also need to establish if it is possible for the school/setting to use the site in the first place as most image hosting sites are free for personal use only. For example many image hosting sites state that they are only intended for personal use and not to be used as generic image hosting service. Professional or corporate uses are often prohibited and this would affect the use of the site and would mean that school use would breach the site terms and conditions.

Schools and settings should undertake appropriate risk assessments 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 by the school/setting to limit any concerns. This would enable the school/setting senior leadership team or management to identify what action to take to safeguard children and staff and to update the school/setting

image policy to ensure that the use of images (such as where the data will be hosted) complies with the Data Protection Act and the school/setting data security policy. Schools and 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 leader, managers, Headteachers and Safeguarding Leads enforce the policy regarding the use of personal phones and devices?

Managers, leaders and headteachers and Safeguarding Leads 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 in order 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). Schools and settings should implement an appropriate acceptable use policy (AUP) which clearly states expectations for safe use as well as any sanctions. Kent County Council provide a template AUP for schools and settings to adapt <http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety>

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

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

Yes. The Data Protection Act 1998 affects the official use of photography by educational settings, as an image of a child is considered to be personal data. It is therefore recommended that written consent is obtained from the parent of a child or young person under the age of 12 (or from the child him or herself if deemed to be competent to make such judgements from 12 years old as suggested by the Information Commissioner) 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?

Schools and settings must get written consent from the parent, guardian or carer of a child or young person up to the age of 18. 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. 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 particular 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.

In exceptional circumstances you may need to make a decision based on the individual case. For example, if a young person has left home but is under 18 years of age, it might be difficult to obtain parental consent. You should also exercise caution when dealing with looked after children and it may be appropriate to get consent from the carer, as well as the child or young person.

Schools/settings will 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) appearing in them leaves the school/setting, so it is recommended that schools/settings destroy them immediately or obtain separate consent to continue to use the image for official purposes.

## Do we need to obtain consent before taking photographs for school /setting administration purposes, e.g. for school/setting trips or SIMS (Information Management System) records?

As long as 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) may make a complaint against the data controller to the Information Commissioner. In some cases this has resulted in prosecution and damages being awarded to the person in the photograph.

## Can we use existing images?

Schools/setting 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 Act 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 e.g. on our website?

We recommend that school/setting websites avoid using:

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

If schools/setting uses a photograph of an individual child, then 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 avoid the risk of inappropriate and unwelcome attention from people outside the school/setting.

As an alternative, settings could ask children to draw a picture of a child or member of staff for the website. Additionally, schools/settings could consider using group or class photographs with very general labels such as "a science lesson" or "making Christmas decorations". Schools/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?

Schools and 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 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

## What if something goes wrong?

The Information Commissioner's Office has the power to impose heavy fines (up to £500,000) on Data Controllers for breaching the 7th principle of the Data Protection Act, which states that 'appropriate security measures must be taken to protect personal information against unauthorised or illegal data processing'.

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

Here are a few examples of undertakings that have been signed recently by schools:

1. A complaint about the way in which **Phoenix 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). [View the Phoenix Nursery School undertaking](#)
2. An undertaking to comply with the seventh data protection principle has been signed by **Holly Park 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. [View the Holly Park School undertaking](#)
3. An undertaking to comply with the seventh data protection principle has been signed by **Bay House 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. [View the Bay House School undertaking here](#)
4. An undertaking to comply with the seventh data protection principle has been signed by **Cherubs Community Playgroup**. This follows the theft of an unencrypted laptop containing personal information relating to approximately 47 families. [View the Cherubs Community Playgroup undertaking](#)
5. An undertaking to comply with the seventh data protection principle has been signed by **Surbiton Children's Centre Nursery**. This follows the theft of a teacher's bag containing an unencrypted memory stick and paperwork. [View the Surbiton Children's Centre Nursery undertaking](#)

You need to consider whether or not you should report any breach to the ICO. There is an expectation that a breach involving highly sensitive personal data or information relating to a large amount of data subjects should be reported.

Below are links to the ICO guidance on data protection breaches

- [http://www.ico.gov.uk/for\\_organisations/data\\_protection/the\\_guide/principle\\_7.aspx](http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx)
- [http://www.ico.gov.uk/for\\_organisations/data\\_protection/~/\\_media/documents/library/Data\\_Protection/Practical\\_application/GUIDANCE\\_ON\\_DATA\\_SECURITY\\_BREACH\\_MANAGEMENT.ashx](http://www.ico.gov.uk/for_organisations/data_protection/~/_media/documents/library/Data_Protection/Practical_application/GUIDANCE_ON_DATA_SECURITY_BREACH_MANAGEMENT.ashx)
- [http://www.ico.gov.uk/for\\_organisations/data\\_protection/the\\_guide/~/\\_media/documents/library/Data\\_Protection/Practical\\_application/BREACH\\_REPORTING.ashx](http://www.ico.gov.uk/for_organisations/data_protection/the_guide/~/_media/documents/library/Data_Protection/Practical_application/BREACH_REPORTING.ashx)

## What should I do if I am concerned about current practise in my school/setting?

If schools or settings are unsure of their legal responsibilities in relation to the use of images then 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 school/setting community should be reported to the school's/setting's designated safeguarding lead (DSL) who may then consult with Kent County Council (the Education Safeguards Team), Social Services or the police, if appropriate.

# Supporting Advice and Guidance

The following information has been provided to ensure that schools, early years providers and other education settings are able to make appropriate and informed decisions in relation to the use of images and videos.

## Legislation and Consent

The Data Protection Act 1998 affects the official use of photography by all educational settings. This is because an image of a child is considered to be 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 12 (or from the child him or herself if deemed to be competent to make such judgements from 12 years old as suggested by the Information Commissioner) 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.

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. Although common in newspapers, the publishing of children's names with their images is not acceptable. Published images could be reused, particularly if large images of individual children are shown.

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. Information about safe usage of new technology can be found at [www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety](http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety)

Settings should recognise that some children, young people and adults will be more vulnerable than others, for example disabled children, Looked After Children (LAC), 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 will be seen as 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 schools/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 KCC with regards to identifying children and young people is as follows

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

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

If a school/setting wishes to **fully** name children in any published text, whether in the school/setting's brochure, website, or in the local press, then it is recommended that they avoid using their photograph unless they have specific written parental consent to do so.

## Use of Photos/Videos by Parents/Carers

Under the Data Protection Act 1998 any photos taken for official setting use may be covered by the Act and parents/carers and children should be advised why they are being taken. Any photos taken purely for personal use (e.g. by parents/carers at events to put into a family album) are exempt from the Act.

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. This right could be implemented should it be deemed appropriate. 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 early years 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 always should 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 indecent/illegal images of themselves or other children (such as images which may show friends or other children in a state of undress). This should be discouraged as it could potentially lead to criminal offences occurring and could place the setting in very difficult situations, 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 then 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, then they will be covered under the Data Protection Act which means parental 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 also ensure that they role model positive behaviour to the children by encouraging them to ask permission before they take any photos. These photos should then be carefully controlled by the setting and checked carefully 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 nursery only (not shared online or via any website or social media tool). This is extremely important to safeguard

vulnerable children e.g. adopted or looked after children. If parents/carers do not give consent for their children's images to be taken in this way, then the setting must ensure those wishes are followed and that images are not taken.

Schools and settings will have their own policies on use of personal devices by children and young people such as mobile phones, camera phones and digital cameras. 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. For advice and guidance relating to the use of personal devices, settings can access the e-Safety policy templates at [www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety](http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety)

## Storage of Images and Videos

Should images need to be kept for a short period of time, they must be protectively stored and password protected on a work computer hard drive or other appropriately encrypted storage device. 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. Express permission must be obtained from the 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 leader/managers must ensure appropriate written parental consent is obtained and that the school/setting have responsibility for the uploading and distribution. Further advice regarding the use of apps to track progress and share images is available in section 7.4 of the KCC Online Safety Policy Template.

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 the Data Protection Act 1998.

## 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 enjoy 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/carer 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 manner in which 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 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 up sports photography.

## Use of External Photographers or Videographers

Any external photographers (including volunteers) who are engaged to record or photograph any events on behalf of the school/setting must be prepared to work according to the terms of the school/setting online safety policy and 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 Data Protection Act 1998.
- 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 which will aim to ensure:

- Compliance with the Data Protection Act 1998
- That images:
  - are only to be used for a specified purpose and will not be used in any other context.
  - 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/carer permission.

Only reputable photography agencies and/or professional photographers should be used by the setting. Details of any checks regarding suitability, which would include 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.

Schools and 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 data protection legislation. Some settings have required volunteers to only use school 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 to the CCTV Code of Practice from the Information Commissioner's Office. The Code of Practice was updated in 2016 and provides guidance and

advice for CCTV users on how to comply with the Data Protection Act 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. When you renew your ICO registration, it would be an appropriate time to consider this. It might be helpful to carry out a Privacy Impact Assessment (PIA) as mentioned on page 9.

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 followed at all times. 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 would be in agreement 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 then the regulations which apply to web-cams 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/setting intent 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.

Schools and 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.

Schools and 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.

<b>Date photograph taken</b>	<b>Length of copyright</b>
Before 1912	Expired
1 July 1912 - 1 June 1957	50 years from the end of the year in which the photograph was taken
1 June 1957 - 1 August 1989	70 years from when the negative was taken
After 1 August 1989	70 years after the death of the photographer

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

More information on copyright is available from the following

United Kingdom's Copyright Licensing Agency: <http://www.cla.co.uk/>

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



# Sample Image Use Policy for Educational Settings

## XXXXX Image Use Policy

**Policy written by:** Nichola Costello

**Approved by Governing Body on:**

**Date to be reviewed:** March 2019

**School Data Controller:** Nichola Costello

**School Designated Safeguarding Lead (DSL):** Nichola Costello

**Governor with lead responsibility:** Mark Gosden

### Official use of Images/Videos of Children by the School/Setting

#### **Scope and aims of the policy**

- This policy seeks to ensure that images and videos taken within and by Frittenden CEP 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 the school.
- All images taken by the school/setting will be used in a manner respectful of the eight Data Protection Principles (Data Protection Act 1998). This means that images will be:
  - fairly and lawfully processed
  - processed for limited, specifically stated purposes only
  - used in a way that is adequate, relevant and not excessive
  - accurate and up to date
  - kept on file for no longer than is necessary
  - processed in line with an individual's legal rights
  - kept securely
  - adequately protected if transferred to other countries
- The Data Controller/DSL and Management team is responsible for ensuring the acceptable, safe use and storage of all camera technology and images within the setting/school. This includes the management, implementation, monitoring and review of the School/Settings Image Use Policy.

## **Parental Consent**

- Written permission from parents or carers will always be obtained before images/videos of children are taken, used or published by the school/setting.
- 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 at the beginning of the pupils education at Frittenden.
- 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/setting will take place using school/setting provided equipment and devices.
- Staff will receive information regarding the safe and appropriate use of images as part of their safeguarding training and responsibilities.
- 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 (Data Controller 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 at all times, unless prior explicit consent has been given by both Data Controller 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 (e.g. with appropriate encryption).
- Any memory stick, CD or storage device containing images of children to be taken offsite for further work will be suitably encrypted and will be logged in and out by the Data Controller and/or DSL and this will be monitored to ensure that it is returned within the expected time scale.
- The Data Controller and/or DSL reserve the right to view any images taken and/or to withdraw or modify a member of staffs' authorisation to take or make images at any time.
- Only official setting owned equipment (e.g. work provided digital or video cameras) will be used by staff to capture images of children for official purposes. Use of personal cameras by staff is prohibited at all times.
- 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/setting will ensure that images always are held in accordance with the Data Protection Act 1998 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 to be taken of any images without relevant authority and consent from the Data Controller and/or DSL and the parent/carers

### **Publication and sharing of images and videos**

- Images or videos that include children will be selected carefully for use e.g. 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 (e.g. newsletters, social media channels) in association with photographs or videos.
- The school/setting will not include any personal addresses, emails, telephone numbers, fax numbers on video, on the website, in a prospectus or in other printed publications.

### **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/setting 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 Closed-Circuit Television (CCTV)**

- All areas which are covered by CCTV will be well signposted, and notifications are displayed so that individuals are advised before entering such vicinity.
- Recordings will be retained for a limited time period only and for no longer than their intended purpose. This will generally be a maximum of 30 days. All recordings are to be erased before disposal.
- Regular auditing of any stored images will be undertaken by the Data Controller and/or DSL or other member of staff as designated by the management team.
- If cameras record activities taking place on the premises which are of a criminal nature or give any cause for concern, then information will be referred to the appropriate agency.
- CCTV cameras will be appropriately placed within the setting.

### **Use of Images/Videos of Children by Others**

#### **Use of Photos/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/setting on health and safety grounds.
- Parents/carers are only permitted to take or make recording within designated areas of the school/setting. 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/setting Data Controller/DSL to discuss any concerns regarding the use of images.

- Photos and videos taken by the school/setting and shared with parents should not be shared elsewhere (e.g. posted on social media site), 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 setting 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 (e.g. unsupervised areas, toilets etc.).
- The use of personal devices e.g. mobile phones, tablets, children's own digital cameras, is covered within the school/settings 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 the Data Protection Act 1998.
- 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 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).
- Photos taken by children for official use will be carefully controlled by the setting 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 (e.g. 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 Professional Photographers**

- Professional photographers who are engaged to record any events will be prepared to work according to the terms of the settings e-Safety policy.
- Photographers will sign an agreement which ensures compliance with the Data Protection Act and that images 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 derive great pleasure from 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 in order to give properly considered consent. It is important that parents/carers and schools/settings have the opportunity to 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. We have had cases in Kent 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 in order to make an informed decision.

## What about school/setting websites?

The same concerns apply to school/setting controlled online sites and there is an added concern that images of children may be copied directly from a site which can then be manipulated or changed by another person. Settings/schools can copy protect images and use lower quality images which means they cannot be usefully enlarged but this can be bypassed so must not be relied upon to keep images safe.

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

Taking pictures or recordings of your own children for your own personal use is ok. The difficulty arises when other children are also to 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 are 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/setting website without appropriate permission from the school/setting.

# Letter Template - Parental Consent for Images

## Dear Parent/carer

This letter explains why we will need to ask for your consent before we are able to take photographs of your child during their time at Frittenden CEP School.

Generally photographs are a source of pleasure and pride. We believe that the taking and use of photographs can enhance the self-esteem of children and their families and therefore is something to be welcomed and appreciated.

We may take photographs for a number of reasons whilst your child is with us, including:

- documenting and recording education activities
- recording their learning and development progress
- recording and celebrating special events and achievements

We will also encourage children to be active learners, and to become involved in using cameras themselves by taking photos of their surroundings, activities and of each other.

We do however recognise that with the increase use of technologies, particularly digitally and online, the potential for misuse has become greater and we understand that this can give rise to concern. We will therefore endeavour to put effective safeguards in place to protect children and young people by minimising risk.

We are mindful of the fact that some families may have reasons why protecting a child's identity is a matter of particular anxiety. If you have special circumstances either now or at any time in the future which would affect your position regarding consent, please let us know immediately in writing.

We have a specific policy regarding the use of images and also include the safe use of mobile phones and personal devices as part of our online safety policy, which you are welcome to view or take a copy of at any time.

To comply with the Data Protection Act 1988, we need your permission before we can photograph or make any recordings of your child. If your child is old enough to express their own view, you may want to consult with them about categories of consent, and we invite you to use this letter to explore their feelings about being photographed at the setting.

Please read and complete the attached forms and do not hesitate to contact me should you have any queries.

Yours sincerely,

Headteacher

# Template Parental Consent Form for Images

- This form is valid for the period of time your child attends Frittenden CEP School The consent will automatically expire after this time. We will not re-use any photographs or recordings after your child leaves the school/setting without additional consent.
- We will not use the personal information or full names (which means first name and surname) of any child or adult in a photographic image or video on our website, online, in our prospectus or in any of our other printed publications.
- If we use photographs of individual children, then we will not use the full name of that child in the accompanying text or photo caption. If we name a child in any text then we will not use a photograph of that child to accompany the article.
- We may include pictures of children and staff that have been drawn by the children. We may use group photographs or footage with general labels. We will only use images of children who are suitably dressed.
- We will discuss the use of images with children in an age appropriate way and to role model positive behaviour.
- This consent can be withdrawn by parent/carer at any time by informing Frittenden CEP School in writing.

	Please Circle as Appropriate
May we use your child's photograph/image in displays around the school/setting?	Yes / No
May we record your child's image or use videos for assessments, monitoring or other educational uses within the school/ setting? These images or recordings will be used internally only.	Yes / No
May we use your child's photograph/image in our prospectus and other printed publications that we produce for educational and promotional purposes?	Yes / No
May we use your child's image on our website or other electronic communications?	Yes / No
May we record your child's image on webcam for appropriate curriculum purposes?	Yes / No
Are you happy for your child to appear in the media e.g. if a newspaper photographer or television film crew attend an event organised by the setting?	Yes / No
Are you happy for the school to print images of your child electronically?	Yes / No

- I have read and understood the conditions of use and I am also aware of the following:
  - Websites can be viewed worldwide and not just in the United Kingdom where UK law applies.
  - The press are exempt from the Data Protection Act and may want to include the names and personal details of children and adults in the media.
- I/we will discuss the use of images with our child/ren to obtain their views, if appropriate.
- As the child's parents/guardians, we/I agree that if we/I take photographs or video recordings of our child/ren which include other children, then we will only use these for our personal use.

Name of Child:

Date:

Parent/Carer Name:

Parent/carer's signature:

Childs Signature (if appropriate):

# Template Group Activity Letter and Form

Dear Parent/Carer

We are staging a production/special event of on xxxxxx. We are sure some parents/carers would like to take photographs/videos of the production. As you know we have a policy in place with regards to the taking, making and use of images and you will have previously signed a consent form stating whether or not your child could be photographed. In circumstances, such as productions or special events, we request specific consent before photographs can be taken by a third party. If you wish to take photos at the production there is a strong possibility that other children will also be included within the picture. We therefore need to ensure all parents/carers who have children in the production are happy for photographs to be taken, and hence need to request their permission.

We all enjoy and treasure images of our family and friends; family events, holidays and events are moments we all like to capture in photos or on video. We now have the exciting dimension of adding our images and videos to our online social networks. This means that we can easily share our photos and video with family and friends. Whilst this can be very useful to all of us we must ensure we protect and safeguard all children and staff, including those who do not want to have their images stored online.

- Some children are at risk and **MUST NOT** have their image put online. Not all members of the community will know who they are.
  - Once posted and shared online any image or video can be copied and will stay online forever.
  - Some people do not want their images online for personal or religious reasons.
  - Some children and staff may have a complex family background which means that sharing their image online can have unforeseen consequences.
- Therefore in order to keep all members of the community safe we must all **'Think Before We Post'** Online

At Frittenden CEP School we are happy for parents and carers to take photos and video of events for personal use but we request that these images are not distributed or put online. This is to protect all members of the community. Please be aware that parents are not permitted to take photographs or to make a video recording for anything other than their own personal use (e.g. with a view to selling videos of an event).

Should any parent/carers not agree with their child being photographed, we will consider alternative options including:

- restricting who is involved in the production/special event
- staging specific photograph opportunities

Photographs of setting productions are ones which parent/carers tend to treasure. We will therefore only prohibit the use of cameras and videos as a last resort. We hope you will support us in this.

We would, therefore, be very grateful if you would complete the slip at the bottom of this letter and return it to me by (date).

Yours sincerely

Headteacher/Manager

# Parental Consent for Images as part of Group Activity

Child's name:

Date:

I am / am not \* happy for photographs to be taken of the production/special event in which my child is due to appear on **xxxxxx** (date)

(\*Please delete as appropriate)

Parent/Carer Name:

Parent/carer's signature:

Childs Signature (if appropriate):



## Guide to the Use of Images Online

### Using Images Safely and Responsibly

We all enjoy and treasure images of our family and friends; family events, holidays and events are moments we all like to capture in photos or on video. We now have the exciting dimension of adding our images and videos to our online social networks, such as Facebook, YouTube and many other websites. This means that we can easily share our photos and video with family and friends.

Whilst this can be very useful to all of us, we must ensure we protect and safeguard all children and staff, including those who do not want to have their images stored online.

### What should we all think about before posting any images or video online and are there any risks?

- Once posted and shared online any image or video can be copied and will stay online forever.
- Some children are at risk and **MUST NOT** have their image put online. Not all members of the community will know who they are.
- Some people do not want their images online for personal or religious reasons.
- Some children and staff may have a complex family background which means that sharing their image online can have unforeseen consequences.
- Therefore in order to keep all members of the community safe we must all **'Think Before We Post'** Online

**At Frittenden CEP School we are happy for parents and carers to take photos and video of events for personal use but request that these images are not distributed or put online. This is to protect all members of the community.**

We thank you for your support

### Further Information on the Use of Images and video:

- Information Commissioner's Office: <https://ico.org.uk/for-organisations/education/>
- Think U Know: [www.thinkuknow.co.uk/parents](http://www.thinkuknow.co.uk/parents)
- Get Safe Online: [www.getsafeonline.org](http://www.getsafeonline.org)

Adapted from resources developed by the Hertfordshire Schools' e-Safety Team

# **Respect and Care for the Whole Community when taking Photos and Videos**

We are happy for parents and carers to take photos and video of their child for personal use but we request that these images are not distributed or shared online if they contain images of other children, adults or staff without consent. Sharing images of others online may put our community at risk.

Thank you for your support

Headteacher/Manager

Adapted from resources developed by the Hertfordshire Schools' e-Safety Team

# Template Consent form for using photographs of Staff

The school/setting would like to use your photograph for staff recognition purposes. These images will appear on our internal intranet and/or website [www.frittenden.kent.sch.uk](http://www.frittenden.kent.sch.uk). To comply with the Data Protection Act 1998, we need your permission to use photographs of you. Please answer the question below, then sign and date the form where shown. We will not use the images taken, or any other information you provide, for any other purpose.

**Please return the completed form, even if you have chosen not to give your consent, to Donna Kneller**

Please circle  
your answer

May we use your image on our website?

- Website/Intranet, accessible by the setting only
- Website, viewable by anyone in the world.

**Yes / No**

**Yes / No**

*Please confirm that you have read and understand the conditions for use, and the notes relating to the eight principles of the Data Protection Act.*

- I have read and understood the conditions of use.
- I confirm that I understand publication of my picture on the setting website/intranet will mean that my picture will be viewable by those with access to the intranet alongside my job title and work contact details and consent to such processing of my personal data.
- I understand that if my picture and details are placed on the website that potentially this will be accessible by anyone in the world with internet access.

Name:

Signed:

Date:

## Conditions of use

1. This form is valid for two years. Your consent will automatically not apply to any other usage of the photos.
2. Images must only be used in circumstances where consent has been given. Signed consent must be given for images to appear on the intranet and/or website (which is viewable by potentially anyone), or they cannot be published in this way.
3. Under the 1998 Data Protection Act your rights include:
  - a) Your consent (to the publication of your photo) can be withdrawn at any time (principle 1 of the Act)
  - b) Your photo will not be used for any other purpose without your further consent (principle 2 of the Act)
  - c) Your personal data will be accurately maintained and kept up to date (principle 4 of the Act)
  - d) Publication of your photo will cease and all electronic copies will be deleted when you leave the setting (principle 5 of the Act)

## Useful Contacts

Kent County Council's e-Safety Guidance and Information for Education Settings:  
[www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety](http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding/e-safety)

Kent County Council's Access to Information Content  
[www.kelsi.org.uk/school-management/data-and-reporting/access-to-information](http://www.kelsi.org.uk/school-management/data-and-reporting/access-to-information)

Kent County Council Education Safeguards Team Content:  
[www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding](http://www.kelsi.org.uk/support-for-children-and-young-people/child-protection-and-safeguarding)

ATL Help and Advice on CCTV and other surveillance:  
[www.atl.org.uk/help-and-advice/school-and-college/CCTV.asp](http://www.atl.org.uk/help-and-advice/school-and-college/CCTV.asp)

ICO Code of Practise for CCTV:  
<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

ICO Sector Guide for Education:  
[www.ico.gov.uk/for\\_organisations/sector\\_guides/education.aspx](http://www.ico.gov.uk/for_organisations/sector_guides/education.aspx)

ICO Information on Data Protection Act for Organisations:  
[www.ico.gov.uk/for\\_organisations/data\\_protection.aspx](http://www.ico.gov.uk/for_organisations/data_protection.aspx)

United Kingdom's Copyright Licensing Agency: <http://www.cla.co.uk/>

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

# Acknowledgements

**This document is the work of the Kent e-Safety Strategy Group and has been based on the “Policy and Guidance for Kent Schools, Settings and KCC Services on the use of photographic images of children” (2008, 2012) and the Online Safety Policy Template 2016.**

This edition has been the work of:

Rebecca Avery, KCC; Michelle Hunt, KCC; Mike O’Connell, KCC

Additional material has been used and developed with thanks to the following organisations:

Hampshire County Council

Herefordshire Grid for Learning (Schools e-Safety Team)

Information Commissioners Office

South West Grid for Learning

Plymouth County Council (Early Years Toolkit)



# Image Use Policy and Guidance for Educational Setting

Error! Reference source not found.Error! Reference source not found.