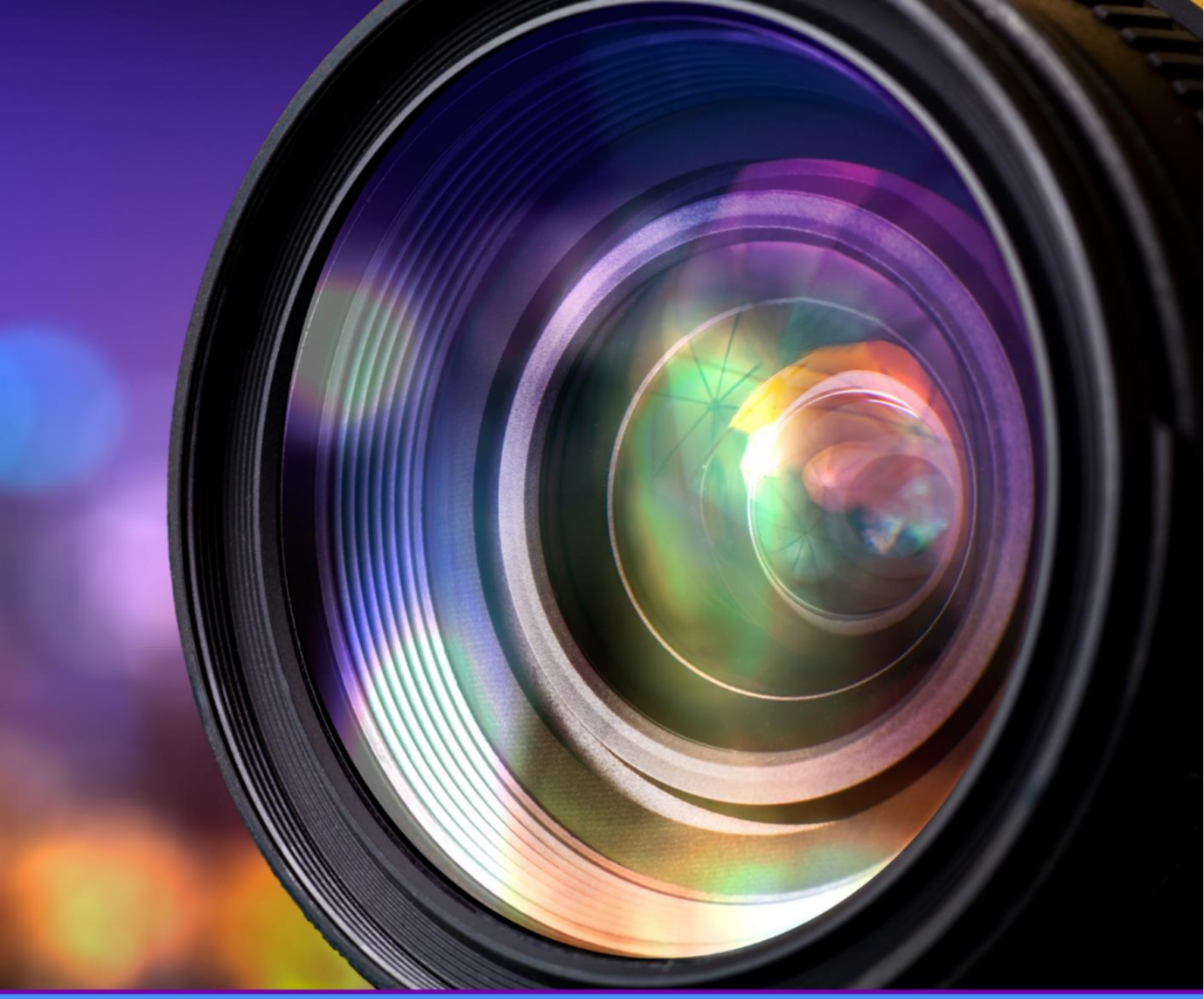

Camera and Image Use Guidance and Template Policy for Education Settings

Guidance for Education Setting Leaders

2023-2024

Kent County Council
kent.gov.uk

Contents

Introduction

This document 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 mobile 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 education 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. Education settings however must be aware that the behaviours of individuals using the technology present the risk, not the technology itself.

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

This document has been developed after discussions between Kent County Council, the press, early year's settings, schools and safeguarding staff. In developing a policy for your own education setting, we suggest that headteachers, 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 concerns must always be able to withhold their consent for image use for whatever reason.

This guidance document and policy template is suitable for education settings including (but not limited to) schools, early years settings, Pupil Referral Units, 14-19 settings, further education colleges, alternative curriculum provisions, Children Centres and hospital schools. 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' within this document, but stress that its use within other education 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

Why do education settings need an image use policy?

Schools, colleges and early years settings 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. Parents/carers specifically need to understand these issues to give properly considered consent. It is also important that parents and settings fully consider the issues before any problems arise.

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

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. 'Keeping Children Safe in Education' (KCSIE) states that schools and colleges 'should *have a clear policy on the use of mobile and smart technology'.*

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 or setting and the full name of a child or adult, then it could be quite easy to find out someone's exact location or address. This 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, for example, families fleeing domestic violence. Education settings may not always be aware of who these vulnerable groups may be. DSLs within education 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. Images are a source and pride for education 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 in Kent of families and staff receiving unwelcome phone calls or visits following appearances in the press or on an education settings website or social media channel. However, this is rare, so it is important to have a sense of proportion. Education settings will want to celebrate success and achievement, but parents/carers should be made aware of the potentially risks in order for them to make informed decisions.

Whilst ultimate responsibility for abuse lies with perpetrators, a staff culture which is complacent (for example, the believe that abuse "couldn't happen here") and unclear, can facilitate an environment whereby abuse is not recognised which places children at 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?

Education setting leaders and managers should ensure that their policies cover 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, mobile/smart phones and wearable technology, including smart watches. 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, headteacher, 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 education 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 Commissioner's Office (ICO). Kent County Council's Access to Information Content can be found on Kelsi.

Do we need written consent to take and use images?

Yes. UK GDPR and Data Protection legislation affects the official use of photography by education settings, as an image 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.

Education settings also need consent from staff and any other adults who may appear in images taken for official use, not just children. A consent form for staff is available in the appendix.

How long does consent last for?

As most children attend settings for a period of time (for example in primary or secondary schools, this is usually five years), it seems sensible to obtain consent for the whole period a child will be attending the setting. Settings also can choose to request consent more frequently, for example, annually. Education 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.

Obtaining consent for a period of time usually means that you won't have to renew parental or child consent until a child changes schools or during transition (for example a young person starts sixth form), however you will have to be careful to record any changed circumstances. This will be easier if you keep images and signed consent forms together.

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

What if we publish an image without obtaining consent?

If you publish an image without consent, then the parent, or child if they have enough 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 image.

Do we need to obtain consent before taking photographs for education setting administration purposes, for example, for trips or SIMS (Information Management 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.

Can we use existing images?

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

If consent was never obtained, for example, images 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 images, it may be helpful to consider the following:

- For what purpose was the image originally taken, for example, was it taken for a specific project such as your school/setting prospectus?
- Where was the image taken, for example was it taken in a public place?
- When was it taken, for example, was it taken recently or a long time ago?
    - Although Data Protection does not relate to deceased people, we should still give their personal data (images in this instance) the same amount of confidentiality.

If a parent, child or young person or member of staff supplies your setting with an image, then you should not automatically assume they are giving their consent to subsequent publishing. Ensure you have a signed consent form before publishing those images 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 education settings' websites and social media channels avoid using:

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

If education settings use a photograph or video of an individual child, they should not include that child's full name in the accompanying text or caption. If a child is fully named in the text, then it is recommended that settings don't include a photograph or video 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 or footage with general labels such as "a science lesson" or "making Christmas decorations". Education settings must remember that they must always get explicit consent, which means getting a signature, before publishing an image of a child or adult, online.

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

The safest approach is to completely avoid staff using any personal equipment or devices to take or share photos or recordings of children, and to always use setting provided equipment channels, even if members of staff believe that individual children cannot be identified.

Use of personal devices can pose data protection risks and can undermine the wider safeguarding culture within a setting. A potential risk of permitting staff to use personal devices to take images is increased danger of allegations following a misinterpreted or misunderstood action; with a personal device it would be more difficult to prove that this was not the case. Allowing use of personal devices can sadly provide opportunities for offenders, however it should be recognised that a ban on using personal devices alone will not prevent this risk. Risk to children and staff is also significantly increased if settings do not have clear and explicit policies in place which are known and understood by all.

When using officially provided equipment, protection is increased for both children and staff. Many education 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. Education settings should implement clear policies and procedures to avoid misuse of work provided devices, for example, password protected, only used by staff, only used for approved/work purposes.

If education settings decide to permit the use of personal devices by staff to take photos or videos of children for work purposes, such in emergency circumstances, this practice should be formally considered and evaluated by leadership, including the DPO and the DSL. The decision by the education settings management regarding this approach should be clearly and formally risk assessed, documented within appropriate policies and explicitly monitored by the DSL and DPO.

Leaders and managers should ensure there are clear and documented boundaries and procedures in place to ensure that data protection legislation is followed, and that children and staff are appropriately safeguarded from harm or potential allegations.

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 or video. 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 smartphones or tablets.

Care must be taken that photographs and videos are stored appropriately. For instance, if staff copy photographs or videos 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 which could lead to a Data Protection breach. Work provided and secure memory cards, remote access systems, memory sticks and CDs should only provide a temporary storage medium and images 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 images 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 so settings should therefore take steps to suitably protect images, for example password protection.

Many settings upload images to third party websites for printing purposes; digital printing can often be cheaper and offer more secure 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, for example, by reading the websites terms and conditions and privacy policy. Education 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.
Education 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 image and it could be used externally for promotion and publicity purposes without the setting’s consent or knowledge. Education settings should ensure they read the terms and conditions and privacy policy of any websites, platforms or apps they are using to identify if this is a risk. Education settings may need to modify their image consent form accordingly to cover third party hosting or usage. It is recommended that any images are suitably protected so that they could not be used without the setting’s, and parents’, consent and knowledge.

Education 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.

Education settings should undertake a Data Protection Privacy Impact Assessment (DPIA) on any websites or apps 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. Education 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.

What about video surveillance (including CCTV)?

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

As with photographs, you must tell the person:

- Why the video surveillance/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 video surveillance can be accessed via its website.

What about images shared when taking part in remote learning?

Where children are being asked to learn online at home they should do so safely. As part of ensuring safe remote learning approaches, settings should give consideration as to how children and staffs images will be used as whilst this can provide benefits to the learning experience, it can pose risks. This includes the possibility of images being captured and shared without permission outside of the remote learning context - this could lead to vulnerable children and/or staff being identified or issues relating to bullying and harassment. Settings may find it helpful to evaluate if the use of images is essential for all members of the community when providing remote learning; in some cases, for example younger learners or vulnerable members of the community, alternatives may be appropriate, for example the use of voiceovers.

Any personal data (including images) which may be captured or shared by settings and/or staff when delivering remote learning must be processed and stored with appropriate consent and in accordance with data protection requirements, for example UK GDPR and any relevant policies. This includes images shared when undertaking remote learning, for example live streamed or pre-recorded videos.

If setting opt to 'record' live streamed sessions, all participants should be made aware that the session is being formally recorded. Recordings should be kept, stored and accessed in line with

existing data protection requirements. Robust risk assessments and up-to-date policies and procedures which outline action taken by the setting to ensure legislation and guidance is complied with should be in place. Local and national guidance on remote learning and a variety of template policies which settings may find helpful to use and adapt can be found on the Education People website.

Can education settings share images with parents/carers?

Education 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 should not be used for official business or for sharing images with parents; this can pose 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 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, videos and text. If settings are considering using such apps, leaders and managers need to 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 should be provided with clear boundaries regarding safe and appropriate use prior to accessing the service/system. Schools and settings should be aware that leaders and managers are ultimately responsible for the security of any data or images held of children.

Education 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 will 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, Headteachers, managers or leaders should carry at 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 DPIAs on its website.

Can education settings share events or performances online?

The following advice has been adapted from the SWGfL guidance which explores how to manage live or pre-recorded events safely, including example parent notifications.

Online live streaming or video sharing platforms provide exciting opportunities for settings to share events with their wider community, for example streaming an assembly, sporting event or nativity play with parents/carers who are unable to attend in person. However, it is not always possible to prevent the forwarding or sharing of images and live streams once they are in the public domain, so settings need to understand and address the possible risks, especially where vulnerable children and/or people outside of the setting community may be involved.

There are a number of ways to share events online including live streaming or pre-recording and sharing content through video hosting or social media platforms (for example YouTube, Facebook), or by using dedicated, and usually restricted setting-controlled platforms, for example remote learning platforms, or the settings official website. The best option will vary based on the type of performance, technology available and settings specific context. An audio-recording or pre-recorded video for example, available via a login on the setting website may be a safer approach for settings with a large proportion of vulnerable children.

If settings opt to broadcast events online, leaders should ensure robust risk assessments have been undertaken before the event takes place to ensure appropriate action can be taken to reduce risks. This will include ensuring the setting has informed and explicit consent from parents and/or children to take part in the broadcast, updating image use and safeguarding policies to ensure this use is addressed and ensuring clear behaviour expectations are in place for children, staff and parents/carers.

Settings should consider the following questions when considering broadcasting events online:

- *Has a risk assessment of the planned activity and platform been used been carried out?* We recommend risk assessments have input from the DSL and DPO and technical staff as well as any staff organising events and are formally approved by the headteacher/manager.
- *What technology is available and/or required and what action needs to be taken to ensure the safety and security of use?* For example, using work provided equipment/accounts only and where social media sites are used, considering if there are any age restrictions or concerns about data protection or privacy.
- *Do you have written consent from parents/children/staff for their participation and imagery to be used in this way?*
- *Do you have all required legal documents for any performances e.g. copyright for any music used, broadcasting license etc?*
- *What steps have been taken to protect the identity of vulnerable children?*
- *What steps have been taken to protect any other people (for example staff or members of the public) who may be featured?*
- *What expectations are communicated to audience members to ensure the safety of the images?* For example, requests not to share a viewing/ listening link with anyone else, if

screenshots, private recordings and wider sharing of the broadcast is allowed and timeframes for the availability of recordings after the event.

- If the event is being recorded:
    - *Do parents/ children/ staff understand the purpose of recording and still consent to participation?*
    - *How long will this be retained for?*
    - *How will the recording be shared?*

It is strongly recommended that staff use setting provided equipment and/or setting approved official communication channels. It is also strongly recommended that any links to events or performances, whether live or pre-recorded, are only shared with an audience known to the setting and require a password or log in to prevent the onward sharing of the broadcast.

Can parents/carers 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. Education 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 of Technology Policy (AUP); this should be shared along with the expectations regarding confidentially and safeguarding etc. with any volunteers before attending or supporting events. Template AUPs are available on the Education People website.

Can parents or staff volunteer to take photos or videos 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 issues that can occur.

Can education settings ban mobile phones and personal devices?

This decision is down to individual leaders and managers based on their specific context and needs, however, a policy which seeks to completely prohibit children, parents and staff from having or using mobile devices, including phones and cameras is likely to be viewed as unreasonable and unrealistic and complete bans can often lead to a culture of suspicion, uncertainty and secrecy. Many staff and visitors would be concerned for health and safety reasons if they were not allowed to carry a mobile phone as they may be used to stay in touch with colleagues, family members or be required for legitimate work purposes.

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 themselves from allegations. Template policies regarding mobile and smart technology including phones and other personal devices are available on the Education People website.

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). Education settings should implement an 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 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 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.

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.

You must 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. The ICO website has further information on fees.

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 UK 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 of course 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 **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).
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.
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.
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.
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.

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-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

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

If education settings are unsure of their legal responsibilities in relation to the use of images, they can consult with the relevant person from any Commissioned Services (for example, if settings purchase data protection advice and/or personnel advice) and their Local Authority, for example information governance services and/or education safeguarding services.

Any evidence of the use of inappropriate images, or the misuse of images by any member of the community should be reported to the education settings Designated Safeguarding Lead (DSL) and Data Protection Officer (DPO) who may then consult with the ICO, Local Authority, Children's Social Work Services and/or the police, as appropriate.

Supporting Advice and Guidance

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

It is recommended that schools and colleges access the DfE Data protection: toolkit for schools, which aims to schools with data protection activity, including compliance with UK GDPR.

Legislation and consent

UK GDPR and Data Protection legislation impacts on all official use of photography by all education 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 or videos 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 children in care; it may be appropriate to get consent from the foster carer and/or social worker, 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 recordings, settings should 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 images of children and young people

Still and moving images and sound add liveliness and interest to a publication or online activity, particularly when children can be included, nevertheless, the safety and security of staff and children is paramount. Published images could be reused, particularly if large images of individual children are shown. Although common in newspapers, the publishing of children's' full names with their images by education settings is not recommended.

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 images should always be appropriately clothed and written consent should be obtained for all children featured.

There will also be times where organisations will be carrying out off-site activities e.g. activity holidays or education 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 and smart technology, including digital cameras and phones or other devices with cameras built in.

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

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 when capturing images of children at PE or swimming events to maintain modesty, for example, using team tracksuits if appropriate. Settings should be aware that children could be identified by logos or emblems on uniforms.

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 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 image.
- If a child in an image is to be named, the setting should avoid fully naming the child.

We would also recommend that settings use the minimum information and consider whether it is necessary to accompany an image with any personal information, for example, children's names, the year group, and/or 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 images unless they have specific written parental consent to do so.

Use of images by parents/carers

Under UK GDPR and Data Protection legislation any images 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 images taken purely for personal use (such as by parents at events to put into a family album) are exempt from this legislation.

Where parents are permitted to take photographs or video 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 (for example, 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 images by children and young people

Many settings have digital cameras or devices which have in-built cameras that can be used by the children to document their activities, and as part of learning. This can be a useful tool to support children's education; however, the use of devices with 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 places 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 UK 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, for example, unsupervised areas and toilets. Staff should be fully aware of the acceptable use expectations and ensure that children are appropriately supervised. Staff should role model positive behaviour to the children by encouraging them to ask permission before they take any photos or videos. Images should be carefully controlled and checked before sharing with parents/carers online or via digital screens. Cameras and/or devices with cameras provided for use by children and the images themselves should 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, for example, will be for internal use by the setting only and not shared online or via any website or social media tool. This is extremely important to safeguard vulnerable children, such as 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.

Education 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 Polices (AUPs) which cover safe usage and possible consequences of misuse, for example 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 images is a criminal offence and any inappropriate use of photography or filming will result in disciplinary action.

Storage of images

Should images need to be kept for even 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.

- Images 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 must be appropriately risk assessed and the DPO, leader/managers must ensure appropriate consent is obtained and that the education 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 UK GDPR and the Data Protection Act. Settings may need to access records management guidance.

Use of images of children by the media

There may be occasions where members of the press are invited to a planned event to take images 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/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 always be observed.

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 interview, and close sports photography.

Use of external photographers/videographers

Any external photographers or videographers (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 UK GDPR and other Data Protection legislation.
- awareness of their specific responsibilities and accountability in line with UK 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 UK GDPR and data protection legalisation.
    - will only be kept for an agreed length of time and will be disposed of in line with UK GDPR and data protection legalisation.
    - 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.

Details of any checks regarding suitability, which would include awareness of UK GDPR and Data Protection legislation as well as evidence of appropriate checks, for example a valid DBS (Disclosure and Barring Service) check should 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. Education settings which allow volunteers, for example, parents or staff, to formally video or photograph productions or events on behalf of the school (such as to create a video for parents and children) will need to consider if this approach can be managed in accordance with UK 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 video surveillance, including closed-circuit television (CCTV)

Any settings use of video surveillance, including CCTV should be developed in accordance with the Information Commissioner's Office guidance. The ICO website provides guidance and advice for video surveillance users on how to comply with Data Protection legislation and includes a simple checklist for users.

Video surveillance, including CCTV may generally 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 video surveillance, or are reviewing its continued use, they should consider 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 video surveillance 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) as mentioned previously.

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

The use of video surveillance by settings should ensure that any manufacturer's instructions, privacy policies and data protection and information sharing guidelines are understood and 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 for video surveillance. Regardless of whether webcams are being used as a security/safety tool or for an education 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. 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 other video surveillance approaches.

Where webcams are used as part of accessing the curriculum, for example as part of remote learning, as with static images, written consent must be obtained. Before seeking such consent, full details of why webcams are to be used should be provided and 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 or respond to unauthorised access or use.

Copyright

Education settings will need to be aware of copyright implications with any images that they might use from elsewhere, for example online.

It is important to be sure of the copyright position of any image's schools/setting intent to use because 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.

Education settings should be aware that photographs and videos 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 copyright; contractors and freelancers own the first copyright in their work, unless the commissioning contract agrees otherwise.

Education 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 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 settings responsibility to ensure that all photographs and videos 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 Education Settings

<Setting Name > Image Use Policy

(Setting Logo)

Key Details

Settings will need to amend the following content and statements to reflect their individual use of images and any leadership and policy decisions.

Policy written by: (Name, Role)

Approved by Governing Body on: (DD/MM/YY)

Date to be reviewed: (DD/MM/YY) It is recommended that settings review this policy on an annual basis as a minimum and/or following any national/local policy or legislation changes.

School/Setting Data Protection Officer: (Name, Role)

School/Setting Designated Safeguarding Lead (DSL): (Name, Role)

Governor with lead responsibility: Amend as appropriate

Scope and aims of the policy

1. This policy seeks to ensure that images taken within and by <school/setting name> are taken and held legally and the required thought is given to safeguarding all members of the community.

2. 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. **Amend as appropriate**.

3. This policy must be read in conjunction with other relevant policies including, but not limited to; child protection, anti-bullying, behaviour, data security, image use, Acceptable Use of Technology Policies (AUPs), confidentiality and relevant curriculum policies including computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE). **Amend as appropriate.**

4. This policy applies to all images, including still photographs and video content taken by <school/setting name>.

5. All images taken by <school/setting name>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

6. The Data Protection Officer (DPO) within the setting (name, role) supported by the Designated Safeguarding Lead (name, role) 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.

Official use of images of children

Parental consent

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

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

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

10. Parental permission will be sought on an agreed basis. **Include specific details, for example, annually or on admission to the setting/school**.

11. 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

12. All images taken and processed by or on behalf of the school/setting will take place using school/setting provided equipment and devices and in line with this and other associated policies, including but not limited to Child Protection, Staff Behaviour/Code of Conduct. **Amend and include other policies as appropriate**.

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

- only publish images of learners where they and their parent/carer have given explicit written consent to do so.
- only take images where the child is happy for them to do so.
- ensure that a senior member of staff is aware that the equipment is being used and for what purpose.
- avoid making images in a one-to-one situation.

- Staff will not
  - take images of learners for their personal use.
  - display or distribute images of learners unless they are sure that they have parental consent to do so (and, where appropriate, consent from the child).
  - take images of learners using personal equipment. **Note: If headteachers/managers opt to allow staff to use personal equipment to take photos/videos of children then clear boundaries and expectations should be detailed, for example, how what circumstances are/are not permitted, how imagery will be stored/deleted etc. and how staff should report any concerns. This is essential in order to safeguard all members of the community.**
  - take images of learners in a state of undress or semi-undress or which could be considered as indecent or sexual
  - take images of a child's injury, bruising or similar or make audio recordings of a child's disclosure.

14. 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.

15. Images will only be retained when there is a clear and agreed purpose for doing so. (Name) designated member of staff (**this should be the DPO or DSL**) will ensure that all images are permanently wiped from memory cards, computer hard and portable drives or other relevant devices once the images will no longer be of use.

16. Images will be stored in an appropriately secure place. **List details**.

17. Images will in the school/setting remain on site, unless prior explicit consent has been given by the DPO and DSL and the parent/carer of any child or young person captured in any images. Should permission be given to take images off site, all relevant details will to be recorded, for example who, what, when and why. Images taken offsite will be kept securely for example with appropriate protection.

18. Any memory stick/storage or 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.

19. 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.

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

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

22. Images 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 DPO and/or DSL and the parent/carer

Safe Practice when taking images

23. 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.

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

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

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

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

Publication and sharing of images

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

29. 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.

Usage of apps/systems to share images with parents

Remove section if the setting does not use tracking apps

30. The school/setting uses <name of system> to upload and share images of children with parents.

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

32. Images uploaded to <name of system> will only be taken on school/setting devices.

33. All users of <name of system> are advised on safety measures to protect all members of the community, for example, using strong passwords, logging out of systems after use etc.

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

Use of Video Surveillance, including CCTV

Remove section if the setting does not use video surveillance

35. All areas which are covered by video surveillance will be well signposted, and notifications are displayed so that individuals are advised before entering such vicinity.

36. Recordings will be retained for a limited time only and for no longer than their intended purpose; this will be a for a maximum of 30 days **(amend if different)**. All recordings are to be erased before disposal.

37. 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.

38. 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.

39. Video surveillance cameras will be appropriately placed within the setting.

Use of webcams

Remove section if the setting does not use webcams

40. Parental consent will be obtained before webcams will be used within the setting environment for education purposes.

41. Where webcams are used with children to access or engage with education (for example remote learning), images and recording will be held in accordance with the UK General Data Protection Regulations (UK GDPR) and Data Protection Act, and any necessary child protection requirements will be implemented.

42. All areas which are covered by webcams for security or safeguarding purposes (CCTV) will be well signposted, and notifications are displayed so that individuals are advised before entering such vicinity.

43. Where webcams are used for video surveillance purposes, recordings will be retained for a limited time only and for no longer than their intended purpose; this will be a for a maximum of 30 days (**amend if different**). All recordings are to be erased before disposal.

Use of images of children by others

Use of image by parents/carers

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

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

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

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

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

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

50. Photos and videos taken by the school/setting 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 images by children

51. The school/setting will discuss and agree age-appropriate acceptable use rules with children regarding the appropriate use of cameras, such as when engaging in remote learning and when onsite. This will include places children cannot take cameras, for example unsupervised areas, toilets etc.

52. The use of personal devices, for example, mobile phones, tablets, digital cameras, is covered within the school/settings mobile and smart technology policy.

53. 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.

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

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

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

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

Use of images of children by the media

58. 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.

59. 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.

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

61. 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, including videographers and volunteers

62. External photographers who are engaged to record any events officially will be prepared to work according to the terms of our policies, including our child protection policy. **Amend as appropriate.**

63. External photographers will sign an agreement which ensures compliance with UK GDPR and the Data Protection Act.

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

65. External photographers will not have unsupervised access to children and young people

Policy breaches

66. Members of the community should report image use concerns regarding image use or policy breaches in line with existing school/setting policies and procedures. This includes… **Insert expectation, for example, inform the headteacher/manager and what policies to follow, for example, complaints, child protection, whistleblowing and/or behaviour policies.**

67. Following a policy breach, leadership staff will debrief, identify lessons learnt and implement policy changes as required. Action will be taken in line with existing school/setting policies and procedures which may include child protection, anti-bullying, mobile and smart technology, acceptable use and behaviour policies. **Amend as appropriate.**

68. Advice will be sought, and reports will be made to other organisations in accordance with national and local guidance and requirements. For example, where there may have been a data protection breach, the ICO will be contacted, and if an allegation has been made against a member of staff, contact will be made with the Local Authority Designated Officer (LADO).

Frequently Asked Questions for Parents or Carers

Why do we need a policy?

Education settings have always used photographs as a way of highlighting success, celebrating achievements or seeking publicity for fundraising. Families enjoy seeing their loved ones in print or online and ww 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 need to understand these issues to give properly considered consent.

So, what are the risks?

The most highly publicised and worrying risk is that a child who appears in the press or online may become of interest to a sex offender. Locating people through the internet has become extremely easy, so if there is a picture and the name of an education setting together with the full name of a child, it could be possible to find out the child's address or work out their likely route to and from the setting. Additionally, it must be recognised that images of children can easily be copied, manipulated or changed once they are published. There are also other specific groups of children, staff and families whose safety could be put at risk if identified online, for example, those fleeing domestic abuse. To limit these risks, we will take appropriate steps, as outlined in the attached consent form and in our image use policy, to safeguard children and our wider community.

Isn't this just scaremongering?

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

What about our official website or other online channels?

Concerns about identification and images being manipulated apply our controlled websites and social media platforms; we will try to copy protect images we share and will use lower quality images on our website and social media channels, but this can be bypassed.

I want to do my own recording of a school/setting play or 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 filmed, and those images are then shared online. It is important to be aware that some members of our community may be vulnerable or at risk so must not have their image shared online. You may not know who is at risk, so we need everyone's support to protect our community. It's important to role model positive behaviour for children, so please check before posting any images online which contain children other than your own. We also ask you do not copy or share images from our website or other channels, without appropriate permission.

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 mages, including photographs and videos of your child during their time at <school/setting name>.

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

We may take images for many 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 also encourage children to be active learners, and to become involved in using cameras themselves by taking photos or videos of their surroundings, activities and of each other.

We do however recognise that with the increased 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 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 the safe use of mobile and smart technology, including mobile phones and other personal devices as part of our child protection and mobile and smart technology policy (**amend as appropriate**), which you are welcome to view or take a copy of at any time.

To comply with UK General Data Protection Regulations (UK GDPR) and the Data Protection Act, 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,

(Name) Headteacher/Manager

Template Parental Consent Form for Images

Settings will need to amend the following content and statements to reflect their individual leadership and policy decisions.

Parental Consent for Use of Images at <school/setting name>

- This form is valid for the period of time your child attends <school/setting name>. This consent will automatically expire after this time.
- We will not re-use any photographs or recordings after your child leaves the school/setting without requesting additional consent.
- We will not use the personal information or full names (first name and surname) of any child in a photographic image or video on our website, online, on social media, in our prospectus or in any of our other printed publications. If we use photographs or videos of individual children, we will not use the full name of that child in the accompanying text or caption. If we name a child in any text, we will not use an image of that child to accompany the article.
- We may use group photographs or footage with general labels.
- We will only take images of children who are suitably dressed.
- We will discuss the use of images with children in an age-appropriate way and role model positive online behaviour.
- This consent can be withdrawn by parents/carers at any time by informing <school/setting name> in writing.
- All images will be used taken and held in accordance with Data Protection legislation.
- All images will be taken and used in accordance with our Image Use, Child Protection, Acceptable Use, Social Media and Mobile and Smart Technology Policy. **Amend as appropriate**.

Parents/carers are encouraged to discuss any concerns or queries relating to image use with us as part of making informed decisions.

May we use your child's image in displays around the school/setting?	Yes / No
May we use your child's image for assessments, monitoring or other education uses within the school/ setting? These images and/or recordings will be used internally only. **Amend as appropriate, for example, if the setting uses tracking apps.**	Yes / No
May we use your child's image in our prospectus and other printed publications that we produce for education and promotional purposes?	Yes / No
May we use your child's image on our official school/setting website?	Yes / No
May we use your child's image on our official social media channels? **Name the channels, for example any official Facebook pages, YouTube channels**	Yes / No

May we use/record/share your child's image on webcam for appropriate curriculum purpose, for example, video conferencing and/or remote learning? **Amend as appropriate.**	Yes / No
May we use/record/share your child's image as part of online broadcasts of performances and events? **Settings should list details of how they will be broadcast, for example pre-recorded, live streamed and where they will be shared such as the official website, closed platform, official social media channel, and the timeframes for the availability of recordings after the event.**	Yes / No
Are you happy for your child to appear in the media, for example, if a newspaper photographer or television film crew attend an event organised by the school/setting?	Yes / No
Are you happy for the school/setting to print images of your child electronically?	Yes / No

I have read and understood the conditions of image use and I am also aware of the following:

- Websites and social media sites can be viewed worldwide; not just in the United Kingdom where UK law applies.
- The press are exempt from UK GDPR and Data Protection legislation 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/re*n 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 own personal use.

Name of Child: _____ Date: _____

Parent/Carer Name: _____

Parent/carer's signature: _____

Child's Signature (if appropriate): _____

Template Group Activity Letter and Form

Dear Parent/Carer

We are staging a production/special event of name on date. 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 your child could be photographed or filmed.

If you wish to take photos or videos at the production, there is a strong possibility that other children will also be included. We therefore need to ensure all parents/carers who have children in the production are happy for photographs and/or videos to be taken.

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 that 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, an image or video can be copied and could stay online forever.
- Some people do not want their images shared online for personal or religious reasons.
- Some children and staff may have a complex family background, which means that sharing their image online could pose significant safeguarding risks and consequences.

In order to keep all members of the community safe we must all **think before we post** online.

At <school/setting name>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 shared 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 for example, with a view to selling videos of an event.

Should any parent/carer 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 productions are ones which parent/carers tend to treasure; we will therefore only prohibit the use of cameras 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 by (date).

Yours sincerely

(Name)

Headteacher/Manager

Parental consent for images as part of group activity

I understand that whilst the school/setting has requested that parents only take and share images of their own children, it is possible that my child may appear in parents' photographs or videos.

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

(*Please delete as appropriate)

Child's name: _____

Date: _____

Parent/Carer's Name: _____

Parent/carer's signature: _____

Child's Signature (if appropriate): _____

Template Broadcasting Letter and Form

Dear Parent/Carer

We are staging a production/special event on date. This year, we will be sharing event name online. **List details of how this will be achieved, for example, it will be pre-recorded and shared online or live streamed, what platform will be used and any specific times.**

The recording will be available for (**insert details about the timeframes for the availability of recordings after the event or remove if it will be live streamed only).**

As you know we have a policy in place with regards to the taking, making and use of images and you have previously signed a consent form stating whether your child could be photographed or filmed.

We all enjoy and treasure images of our children. Whilst the use of technology to share and access images brings fantastic benefits, we must however ensure that we protect and safeguard all children and staff. Some children are at risk and **MUST NOT** have their image shared online and not all members of our community will know who they are.

In order to keep all members of the community safe we must all think before we share online. You can support us in keeping all children safe by: **(amend as appropriate)**

- Remembering images and videos shared with you by the school/setting are for your own or your family's personal use only.
- Thinking about who has the right to view or listen to the recordings, not only of your own child, but of others who will have been included as well.
- Considering whether or not to share this imagery online. If you choose to do so then you must make sure this is limited to immediate family only and not made publicly available.
- **Include any setting expectations around taking screenshots, private recordings and wider sharing of the broadcast**

If content is shared or accessed outside of our requested expectations, then we may restrict or prohibit access in the future. Photographs of special events are ones which parent/carers tend to treasure; we will therefore only prohibit access as a last resort. We hope you will support us in this.

We would, be very grateful if you would complete the slip at the bottom of this letter and return it by (date). If you need to discuss any of the points within this letter or have a related image use query, please don't hesitate to contact us to discuss further.

Yours sincerely

(Name)

Headteacher/Manager

Parental consent for children's images being broadcast online

I understand that school/setting will be broadcasting event name online.

The event will be broadcast/recording will be available via insert details e.g. platform, how it can be accessed and specific times if it will be live streamed.

I understand the broadcast will be accessible for insert details about the timeframes for the availability and access to recordings after the event. **Remove if live streaming only**.

I understand that the school/setting has requested that parents/carers:

- Do not share the link or related access information to broadcast events with anyone outside of the immediate family.
- **Include any expectations regarding taking screenshots, private recordings and wider sharing of the broadcast.**

I *am / am not* * happy for my child to be involved in the broadcast of production/special event on (date).

(*Please delete as appropriate)

Child's name: _____

Date: _____

Parent/Carer's Name: _____

Parent/carer's signature: _____

Child's Signature (if appropriate): _____

Posters for Education Setting Use

Setting Logo

<school/setting name> 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 sharing our images and videos to online social networks, such as Facebook, YouTube, WhatsApp and other websites. This means that we can easily share photos and video with family and friends quickly. Whilst this can be useful, we must however ensure that we all take steps to protect and safeguard children and staff, including those who do not want to have their images stored or shared 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 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 and dangerous consequences.
- Some children are at risk and MUST NOT have their image put online; not all members of the community will know who they are.

In order to keep all members of the community safe we must all '**think before we post'** online

At <school/setting name> we are happy for parents and carers to take photos and video of events for personal use but request that these images are not posted or shared 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 and online safety:

- Information Commissioner's Office: https://ico.org.uk
- NCA-CEOP: www.thinkuknow.co.uk/parents
- Get Safe Online: www.getsafeonline.org
- Childnet: www.childnet.com

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

Setting Logo

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 at this event for personal use. We request that these images are not distributed or shared online if they contain 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 (link). To comply with UK General Data Protection Regulations (UK GDPR) and the Data Protection Act, 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 (name of contact).

School/Setting Name Staff Photograph Consent Form

Conditions of use

1. This form is valid for (**Include time frame details, for example, two years from the date of signing or for the time scale of a project only**). 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 UK GDPR and Data Protection legislation 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)

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

Please circle your

	answer
May we use your image on our:	
• School/Setting intranet/learning platform, accessible by the school/setting only?	Yes / No
• Display and notice boards, accessible by the school/setting only?	Yes / No
• Website, viewable by anyone in the world?	Yes / No
• Official social media channels (*list*), viewable by anyone in the world?	Yes / No

Name: _____

Signed: _____

Date: _____

Acknowledgements

This guidance has been written by the Education People's Education Safeguarding Service based on guidance produced with input from the Kent County Council Information Governance Team.

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

Disclaimer