KENT LADO EDUCATION SAFEGUARDING
ADVISORY SERVICE

Image Use Guidance and Policy Template

For Schools and Education Settings

KEEPING CHILDREN SAFE IN THE CHILDREN'S WORKFORCE

Contents

Introduction

This guidance applies to the taking, use, storage and sharing of images and recordings within education settings. This includes photographs, video, livestreaming, webcams, CCTV, mobile phones, tablets, wearable technology, portable gaming devices with inbuilt cameras, and any other digital technology or platforms used to capture, store, print, publish or share images.

Photography and video can provide valuable opportunities for education settings to celebrate achievements, record learning, engage with families and promote the culture of the setting. However, as digital technology has become more accessible and sophisticated, the potential for images to be copied, shared, altered or misused has increased.

Education settings should recognise that the online environment has changed significantly and images published online may now be vulnerable to manipulation and exploitation by offenders using artificial intelligence and other digital tools. Settings should therefore approach decisions about taking, storing and sharing images from a safeguarding and data protection first perspective, rather than solely as a communications, publicity or administrative activity.

This guidance aims to support leaders, governors, proprietors, managers, Designated Safeguarding Leads (DSLs), Data Protection Officers (DPOs) and other staff to make informed, safeguarding-led decisions about image use.

This guidance and policy template is suitable for a range of education settings, including but not limited to schools, early years settings, Pupil Referral Units, 14–19 settings, further education colleges, alternative provision, children's centres, hospital schools and other settings working with children and young people. For simplicity, this document may use terms such as "school" and "pupils" in some places. Education settings will need to amend and adapt the sample materials included in this document to reflect their own context, ethos, community, technology, systems and procedures.

In developing or reviewing an image use policy, settings should involve relevant leaders and staff, including the headteacher or manager, governing body or proprietor, DPO, DSL and any staff responsible for communications, online safety or information governance. Settings may also wish to explain their approach to parents/carers, children and other stakeholders so that expectations are understood by the whole community.

Settings are also encouraged to access and consider the guidance developed by the UK Online Harms Early Warning Working Group, *Protecting your setting's images from AI manipulation and abuse*, which provides further advice on protecting images of children and young people from online misuse.

Any parent/carer, child or member of staff with concerns about image use should be able to raise those concerns and, where consent is being relied upon, withhold or withdraw consent for any reason.

Disclaimer

This guidance and policy template have been developed by Kent County Council's LADO Education Safeguarding Advisory Service (LESAS) to support education settings to make informed, safeguarding-led decisions about the taking, use, storage and sharing of images. If errors or required updates are brought to our attention, we will review and amend the document as soon as practicable.

Every effort has been made to ensure that the information in this document is accurate and up to date at the time of review. However, this document is provided for general guidance only and does not constitute legal advice. Education settings remain responsible for ensuring that their own policies, procedures, records, systems and decisions are appropriate for their context and comply with current legislation, statutory guidance and any relevant local or organisational requirements.

Where settings are unsure about their responsibilities, including in relation to consent, parental responsibility, lawful basis, data protection, copyright, safeguarding concerns, CCTV/video surveillance, use of external platforms or image misuse, they should seek advice from an appropriate professional. This may include their Data Protection Officer (DPO), commissioned data protection or legal service, local authority, safeguarding partners, the Information Commissioner's Office or other relevant specialist support.

This document was last updated and published in June 2026.

Copyright

Frequently Asked Questions

Why do education settings need an image use policy?

Education settings frequently use photographs and videos to celebrate achievements, record learning, communicate with families and promote the life and work of the setting. Parents, carers and children often value seeing these experiences reflected in newsletters, displays, websites and other communications. However, placing images or identifying information into the public domain can create safeguarding, privacy and data protection risks.

This does not mean that settings should stop sharing images altogether. Instead, leaders should robustly risk assess their practice and review whether public sharing remains necessary, proportionate and appropriate. Decisions and expectations regarding image use should be clearly communicated to staff, pupils and parents/carers through their school/setting policies.

Education settings have statutory obligations to ensure that image use complies with data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Section 3 of the statutory framework for the Early Years Foundation Stage (EYFS) from the Department for Education (DfE) states that safeguarding policies must include how mobile phones, cameras and other electronic devices with imaging and sharing capabilities are used within the setting. All settings with foundation stage provision must therefore have policies and procedures which address the safe use of mobile phones, cameras and devices with imaging and sharing capabilities.

Keeping Children Safe in Education (KCSIE), issued by the DfE states that schools and colleges should have a clear policy regarding the use of mobile and smart technology. KCSIE also highlights that governing bodies and proprietors should ensure that personal information is processed lawfully, fairly and securely in line with data protection legislation.

Governing bodies, proprietors and management committees should ensure that image use policies are reviewed regularly and reflect current safeguarding, online safety and data protection risks. Leaders should ensure that decisions regarding image use are not delegated solely to communications or marketing functions and are informed by safeguarding expertise, including input from DSLs and DPOs where appropriate.

Further details on information sharing requirements and expectations can be found at:

- Working Together to Safeguard Children
- Information Sharing: Advice for Practitioners Providing Safeguarding Services to Children, Young People, Parents and Carers
- The Information Commissioner's Office (ICO)
- DfE Data protection in schools

- DfE IT service and digital equipment standards

What are the risks?

Sharing images publicly can create safeguarding, privacy and data protection risks for children, families and staff, particularly where individuals may be identifiable through linked information such as names, uniforms, locations, routines or setting details.

One of the most concerning risks is that images of children or adults may attract the attention of individuals who pose a safeguarding risk, including those who sexually abuse or exploit children. Advances in technology, including artificial intelligence and image manipulation tools, have increased the possibility of publicly available images being copied, altered or misused to create abusive, exploitative or sexualised content.

Images and information shared online may also increase risks relating to:

- online grooming or exploitation
- stalking, harassment or intimidation
- blackmail or extortion attempts
- impersonation or identity misuse
- unwanted contact
- children, families or staff being located or identified offline

Some children and adults may be particularly vulnerable if identified publicly online. This may include:

- children in care
- adopted children
- children subject to safeguarding plans or court orders
- families fleeing domestic abuse
- staff experiencing harassment, stalking or intimidation
- children or adults at increased risk due to personal, cultural, religious or family circumstances

Education settings may not always be aware of every individual who may be vulnerable within their community. DSLs therefore play an important role in ensuring that image use decisions are informed by safeguarding considerations and that risks are assessed appropriately.

At the same time, it is important that settings maintain a balanced and proportionate approach. Most children who experience abuse are harmed by someone known to them, and serious incidents involving image misuse by strangers remain relatively uncommon. Images and videos are often an important way for settings to celebrate achievements, record learning and strengthen communication with families and the wider community. By taking reasonable and proportionate steps to reduce risk, including limiting identifying information, carefully considering whether public sharing is necessary, using safer image choices and ensuring clear policies and procedures are in place, settings can continue to use images in a safer and more informed way.

Why are settings being encouraged to review image sharing practices?

Concerns regarding online image misuse are based on real and evolving safeguarding, privacy and safety risks.

Education settings have long needed to consider the potential risks associated with publicly sharing images and personal information online. However, advances in technology, including artificial intelligence and image manipulation tools, have significantly changed the online environment in which images are shared and accessed.

National agencies including the Internet Watch Foundation and the UK Council for Internet Safety (UKCIS) Online Harms Early Warning Working Group, have highlighted increasing concerns regarding the misuse of publicly available images using artificial intelligence and other digital technologies. Images taken from websites and social media may now be copied, manipulated or reused without consent, including to create abusive, exploitative or synthetic imagery.

While serious incidents remain relatively uncommon, education settings should regularly review whether their image-sharing practices remain necessary, proportionate and appropriate in light of evolving online risks.

The purpose of this guidance is not to prevent settings from celebrating children's achievements or sharing learning experiences. Instead, it is intended to help leaders, governors, managers and DSLs make informed safeguarding decisions regarding when, where and how images are taken, stored and shared.

Settings should carefully consider:

- whether public sharing is necessary
- what level of identifiability is appropriate
- whether safer alternatives are available
- how risks can be reduced
- whether the benefits outweigh potential safeguarding and privacy concerns

This approach supports a safeguarding-first and proportionate response, rather than a blanket ban on image use.

What do leaders need to consider?

Education setting leaders and managers should ensure that their policies clearly set out expectations for the safe, responsible and appropriate use of cameras, mobile phones and devices with imaging and sharing capabilities by children, staff, parents/carers and visitors. Policies should reflect the wide range of devices now capable of capturing and sharing images, including tablets,

mobile and smart phones, wearable technology such as smart watches, webcams and online platforms used to store or share images.

Leaders should ensure that image use is approached as both a safeguarding and data protection issue, rather than solely a communications or operational matter. Decisions regarding the taking, storage and publication of images should be informed by safeguarding, online safety, privacy and proportionality considerations. This is particularly important given the increasing ability for publicly available images to be copied, manipulated or redistributed online without consent.

The image use policy should apply to, and be understood by, all individuals who access, use or manage work-related photographic equipment or images. This may include children and young people, parents and carers, staff, volunteers, governors, students, contractors, visitors and external photographers or media representatives.

Leadership teams are ultimately responsible for ensuring the safe, lawful and appropriate use, storage, sharing and disposal of images and image-related technologies within the setting. This includes ensuring that policies and procedures are regularly reviewed, staff receive appropriate safeguarding and data protection training, and that concerns regarding image misuse are responded to appropriately.

Governing bodies, proprietors and management committees should ensure that image use policies reflect current safeguarding, online safety and data protection expectations, including emerging risks associated with artificial intelligence and image manipulation technologies.

The Headteacher/Manager, DSL and/or DPO should retain oversight of official image use and may request access to official images where appropriate. They may also withdraw or amend authorisation for individuals to take, use or share official images if concerns arise regarding safeguarding, professional conduct, policy compliance or data protection.

All staff should ensure that official images remain available for scrutiny and that they can justify the purpose, storage and use of any images in their possession.

Do we need written consent to take and use images?

Images of identifiable individuals are personal data, so settings must ensure that any use of photographs or videos complies with data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Where images are used for publicity, marketing, websites, social media, prospectuses or other external communications, settings should usually obtain explicit written consent from parents/carers and, where appropriate, involve children and young people in those decisions.

As children mature, settings should talk to them about how their images may be used and take their wishes and feelings into account wherever possible. Consent for image use should not be

treated simply as an administrative task, but as part of a wider safeguarding and privacy process. Parents/carers should be supported to make informed decisions, particularly where images may be shared publicly online.

There will be occasions where settings use images for internal educational, safeguarding, security or administrative purposes. In these situations, settings should ensure there is a clear and appropriate reason for the use of the image, that it is handled securely and that it is only retained for as long as necessary.

Where there is uncertainty regarding consent, parental responsibility or the most appropriate lawful basis for using images, settings should seek advice from their DPO or other relevant professionals.

What if parents/carers disagree about image consent?

Where more than one person has parental responsibility, settings may sometimes receive conflicting views about whether a child's image should be used. For example, one parent/carer may give consent for images to be used, while another refuses consent or later withdraws it.

Where there is disagreement between people with parental responsibility, settings should usually take a cautious approach and treat consent as not having been given for the disputed use. This is especially important where images may be published online, shared on social media, used in publicity materials, provided to the media or otherwise shared outside the setting community.

Settings should record the disagreement clearly, ensure relevant staff are aware of any restrictions, and avoid using the child's image for the disputed purpose unless and until the position is resolved. Records should focus on the consent position, any restrictions and the action agreed. Settings should avoid recording unnecessary details about family circumstances unless this is needed for safeguarding or legal decision making.

Where there is uncertainty about parental responsibility, court orders, safeguarding risks or whether an image can lawfully be used, settings should seek advice from their DPO, DSL, local authority, commissioned legal/data protection service or other relevant professional.

The DfE guidance on parental responsibility for schools states that the welfare of the child must be a school's paramount consideration and that schools should seek legal advice where they are unsure how to act in relation to parental responsibility concerns. Other education settings should take a similarly cautious approach and seek appropriate advice where needed.

How long does consent last for?

As most children attend a setting for several years, many education settings choose to obtain consent for the full period a child is expected to attend, for example throughout primary or secondary education. Other settings may prefer to review and renew consent more regularly, such as annually or at key transition points.

Whichever approach is taken, settings should ensure that consent arrangements are kept under regular review and that any changes in circumstances are recorded promptly. This is particularly important where safeguarding, family or privacy concerns arise during a child's time at the setting.

Parents/carers and, where appropriate, children and young people should be reminded that consent can be withdrawn or amended at any time. Settings should ensure there are clear processes in place for recording and responding to changes in consent.

It is good practice to keep image records and consent information organised and accessible so settings can identify which images can be used, where they have been published and when they should be reviewed or removed.

Settings should not normally continue to use images of children or staff after they have left the setting unless there is a clear reason to do so and appropriate consent remains in place. Images that are no longer required should be securely deleted or destroyed in line with the setting's retention and data protection procedures.

In some circumstances, settings may wish to retain historic images for archiving, historical or commemorative purposes. Where this is the case, settings should ensure this is considered carefully, is proportionate and complies with data protection requirements.

What if we publish an image without obtaining consent?

If a setting publishes or shares an image without appropriate consent, or without another clear lawful basis, this may result in safeguarding, privacy and data protection concerns.

In some situations, the publication of an image could place a child, family member or staff member at risk, particularly where individuals are identifiable or where there are existing safeguarding concerns. It may also cause distress, damage trust between families and the setting, or lead to complaints being raised.

Parents/carers, staff members, or children and young people where appropriate, may raise concerns directly with the setting or make a complaint to the Information Commissioner's Office (ICO). In some circumstances, organisations have faced regulatory action, financial penalties or legal claims relating to the inappropriate use or sharing of personal data, including images.

If a concern arises, settings should act promptly to review the circumstances, remove images where appropriate, assess whether a data breach may have occurred and seek advice from their DPO or other relevant professionals.

The best way to reduce risk is to ensure that clear policies, consent processes and review procedures are in place and understood by the whole setting community.

Can we use existing images?

Education settings may already hold photographs or videos taken in previous years. Before reusing older images, settings should consider whether the original consent remains valid, whether the intended use has changed and whether the image remains appropriate to use in the current context.

For example, if consent was originally obtained for printed publications only, settings should carefully consider whether additional consent should be obtained before using those images online or on social media.

Settings should also recognise that safeguarding circumstances can change over time. An image which may have been considered appropriate to use previously may no longer be suitable due to changes in a child's or family's circumstances, developments in technology or the increased risks associated with public online sharing.

When considering whether to reuse existing images, it may be helpful to consider:

- why the image was originally taken
- how and where it was originally intended to be used
- how long ago it was taken
- whether consent remains valid and appropriate
- whether the image includes identifiable information
- whether the image remains necessary and proportionate to use
- whether the use could create safeguarding, privacy or reputational concerns

Even where data protection legislation may no longer strictly apply, settings should continue to handle historic images sensitively and respectfully.

If a parent/carer, child, young person or member of staff provides an image to the setting, this should not automatically be taken as consent for wider publication or online sharing. Settings should ensure that appropriate consent and permissions are in place before using supplied images in official publications, websites, social media or other communications.

Should we post images of children or staff online, such as on websites or social media?

Education settings should carefully consider whether publicly sharing images of children or staff online is necessary and proportionate.
Images published online may be copied, downloaded, manipulated, redistributed or reused without the setting's knowledge or consent. This includes the potential use of artificial intelligence and other digital tools to create altered, abusive or exploitative content. Once content is publicly accessible online, settings have limited control over how it may subsequently be used. Settings should therefore adopt a safeguarding-first approach to image publication decisions.

Before sharing images publicly, leaders should consider:

- whether public sharing is necessary
- whether a less identifiable image could be used
- whether a restricted platform or parent portal would be safer
- whether the image includes identifying information such as:
    - faces
    - uniforms
    - names
    - locations
    - routines
    - information that could increase risk if shared publicly
- whether the benefits outweigh the safeguarding and privacy risks

Where possible, settings should consider safer alternatives such as:

- images of activities or displays
- over-the-shoulder photographs
- group images taken from a distance
- images where faces are not clearly visible
- illustrations or children's work
- restricted or password-protected sharing methods

Where settings do decide to share images publicly, they should:

- obtain appropriate written consent
- minimise identifying information
- remove metadata where possible
- use lower-resolution images where appropriate
- regularly review and remove images that are no longer required
- ensure staff understand safeguarding and data protection expectations

Education settings should also recognise that staff images may be vulnerable to misuse, impersonation, harassment or manipulation online and should apply the same safeguarding and proportionality principles to staff imagery.

Can staff use their personal phones/cameras to take photos or recordings of children?

The safest approach is generally for staff to avoid using any personal devices to take, store or share photos or recordings of children, and instead to use setting-provided equipment wherever possible.

Using personal devices can create safeguarding, privacy and data protection risks for both children and staff. It may also increase the risk of misunderstandings, allegations or concerns about professional boundaries, particularly where images are stored on personal phones or shared through personal accounts, apps or communication channels.

Education settings should also recognise that personal devices can make it more difficult to monitor, manage or securely remove images where concerns arise. In some cases, individuals who pose a safeguarding risk may seek to misuse personal devices or communication channels to access, store or share images inappropriately. However, settings should recognise that simply banning personal devices alone will not remove these risks; clear policies, professional boundaries and a strong safeguarding culture remain essential.

Where settings provide work devices for taking or storing images, leaders should ensure there are appropriate safeguards in place, such as password protection, restricted access, secure storage and clear expectations regarding acceptable use. Many settings choose to use shared work cameras or dedicated work devices and communication accounts to help reduce risks for both children and staff.

If a setting decides that staff may use personal devices in exceptional circumstances, such as during an emergency or where no suitable alternative is available, this should be carefully considered by leadership teams, including the DSL and DPO. The circumstances in which this may be permitted, and the steps staff must take afterwards, should be clearly documented within policies and understood by all staff.

Leaders and managers should ensure there are clear procedures in place regarding the safe use, storage, transfer and deletion of images, and that staff understand how to report any concerns relating to image use, safeguarding or data protection.

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

Education settings should ensure there are clear procedures regarding when and how images of children may be accessed, stored or transferred off site by staff.

Where possible, images taken for official use should remain within the setting's secure systems and should only be accessed by authorised staff for legitimate professional purposes. Images should not normally be stored on personal devices, personal accounts or unsecured storage systems.
If staff need to access or transfer images off site for legitimate work purposes, settings should ensure that appropriate safeguards are in place. This may include the use of encrypted devices, secure remote access systems, password protection and clear procedures regarding storage, transfer and deletion of images. Images should only be retained for as long as necessary and should be securely uploaded to the setting's approved systems as soon as possible.

Settings should take particular care when using apps, cloud storage systems, third-party platforms or external providers to store, share or print images. Before using such services, leaders should ensure they understand:

- where data will be stored
- who can access it
- how images may be used by the provider

- whether appropriate security arrangements are in place
- whether the terms and conditions permit reuse of uploaded content

Settings should also ensure that any third-party platforms or apps used for storing or sharing images are appropriately risk assessed, including through a Data Protection Impact Assessment (DPIA) where required. The DSL, DPO and leadership team should be involved in these decisions to ensure safeguarding, privacy and data protection risks are appropriately considered.

Where images are shared externally, including with media organisations or printing companies, settings should ensure that secure transfer methods are used and that only trusted and reputable providers are engaged.

Staff should receive regular guidance and training regarding the secure handling, transfer, storage and deletion of images to help ensure that children, families and staff are appropriately safeguarded.

What about video surveillance (including CCTV)?

Some education and early years settings use video surveillance, including CCTV, for a range of purposes such as site security, safeguarding, monitoring access to buildings, supporting safer working practices or investigating incidents or concerns. Some parents, carers and professionals may view CCTV as providing additional reassurance, accountability or oversight within settings.

At the same time, the use of CCTV and digital monitoring in education and early years provision remains an area of ongoing professional discussion. While some view surveillance as a potentially helpful safeguarding measure, others have raised concerns regarding privacy, children's dignity, staff trust, cyber security and the extent to which CCTV can realistically prevent harm. CCTV should therefore not be viewed as a standalone safeguarding solution, but as one part of a wider safeguarding, supervision and safer working culture.

Where video surveillance is in place, settings must ensure that individuals are clearly informed before entering the area. Signage and privacy information should explain why recording is taking place, how recordings will be used, who may access them and how long they will be retained.

Settings should identify and document an appropriate lawful basis for the use of video surveillance and regularly review whether its use remains necessary, proportionate and justified. Leaders should also carefully consider the potential impact of surveillance on children, families and staff, alongside wider safeguarding, supervision, whistleblowing and safer working arrangements within the setting.

DSLs, managers and proprietors may wish to keep their approaches to supervision, escalation processes, safer working practice and safeguarding culture under regular review, regardless of whether CCTV is currently in place.

Further advice regarding CCTV and video surveillance can be accessed via the Information Commissioner's Office (ICO) guidance.

What about images shared when taking part in remote learning?

Where children take part in remote/online learning, settings should consider carefully how images, video and audio will be used. Seeing and hearing others can support engagement, communication and relationships, but it can also create safeguarding, privacy and data protection risks if images are captured, recorded or shared outside the intended learning context.

Settings should consider whether it is necessary for children or staff to be visible on camera and whether safer alternatives could be used. For example, in some circumstances it may be appropriate to use audio only, blurred backgrounds, initials rather than full names, or pre-recorded content which does not identify children. This may be particularly important where children, families or staff may be vulnerable, or where there are concerns about images being copied, screenshotted or shared without permission.

Any images, video or audio captured as part of remote learning should be handled in line with the setting's safeguarding, online safety and data protection policies. Settings should be clear with staff, children and parents/carers about expectations for online sessions, including whether cameras should be used, whether screenshots or private recordings are permitted, how concerns should be reported and what action may be taken if images or recordings are misused.

If a session is being formally recorded by the setting, all participants should be informed in advance. Recordings should only be made where there is a clear purpose, and they should be stored securely, accessed only by authorised individuals and retained only for as long as necessary.

Settings should ensure that remote learning arrangements are risk assessed and reviewed regularly, particularly where live video, recorded sessions, external platforms or third-party providers are used. Staff should also receive clear guidance on safe and appropriate practice when delivering remote learning, including the use of setting-approved devices, accounts and platforms.

Can education settings share images with parents/carers?

Education settings will need to consider the safest and most appropriate way to share images with parents and carers. Sharing photographs or videos can be a positive way to celebrate learning, development and special events, particularly in early years and primary settings. However, settings should carefully consider the method used, the type of images being shared and whether any other children, staff or families may be identifiable.

Where images are shared directly with parents/carers, settings should use approved setting systems, devices and communication channels. Staff should not use personal phones, personal email accounts, personal messaging apps or personal social media accounts to share images for official purposes, as this may create safeguarding, professional boundary and data protection risks.

Many settings use online platforms, apps or learning journals to share children's learning and development with parents/carers. Before using these systems, leaders and managers should understand where children's data and images will be stored, who can access them, how long they will be retained and what the provider's terms and conditions allow. Settings should also consider whether the platform is secure, whether access can be limited appropriately and whether parents/carers understand how the system should be used.
Parents/carers and staff should be given clear expectations before being given access to any app, platform or image-sharing system. This should include expectations about not copying, downloading, screenshotting, altering or sharing images more widely, particularly where images include children other than their own. Once images have been shared with parents/carers, settings may have limited control over how they are used, so it is important that the whole community understands the potential safeguarding and privacy risks.

Where a new system, app or platform is being introduced, settings should consider whether a Data Protection Impact Assessment (DPIA) is required. This should help leaders, the DPO and other relevant staff consider any privacy, safeguarding and security risks before the system is used.

Settings remain responsible for ensuring that images of children are handled safely, lawfully and in line with their own safeguarding, data protection, online safety and image use policies.

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.

Live streaming and video sharing can provide valuable opportunities for settings to include parents, carers and wider family members who may not be able to attend events in person. This might include assemblies, sports days, performances, celebrations or other community events. However, settings should consider carefully whether online sharing is necessary and, if so, what approach would be safest and most proportionate.

Once an event is live streamed, recorded or shared online, it may be difficult to control what happens to the images or footage afterwards. Links may be forwarded, screenshots or private recordings may be taken, and content may be downloaded or shared beyond the intended audience. This can create safeguarding, privacy and data protection risks, particularly where children, staff, families or other individuals may be vulnerable or identifiable.

Settings may choose to share events in different ways, including live streaming, pre-recording content, sharing a recording through a restricted platform, or using an audio-only option. The safest approach will depend on the nature of the event, the children and adults involved, the technology available and the setting's own safeguarding context. For some settings, particularly where there are children or staff who may be at increased risk if identified, a restricted platform or audio-only recording may be more appropriate than a publicly accessible video.

Before sharing any event online, leaders should ensure that the activity has been considered carefully and risk assessed. This should include input from the DSL, DPO, relevant technical staff and those organising the event. Settings should consider whether appropriate consent has been obtained, whether any children or adults need additional protection, how access will be restricted, how long any recording will be available and what expectations will be communicated to viewers.

Parents/carers, staff and children, where appropriate, should be told clearly how the event will be shared, who will be able to access it, whether it will be recorded, how long it will be retained and whether screenshots, private recordings or onward sharing are permitted. Settings should also ensure that any necessary permissions or licences are in place, for example in relation to music, scripts or other copyrighted material.

Where possible, events should be shared using setting-approved equipment, accounts and platforms. Links to live or recorded events should only be shared with an intended audience known to the setting and, wherever possible, should require a password, login or other access control. Public sharing through open social media or video sharing platforms should be carefully considered and only used where leaders are satisfied that the benefits outweigh the safeguarding and privacy risks.

If recordings are made, they should be stored securely, accessed only by authorised individuals and retained only for as long as necessary. Settings should also make clear what action may be taken if access links, images or recordings are shared inappropriately.

Can parents/carers take their own photos or recordings at events?

Parents/carers often want to take photographs or videos of their own children at setting events, such as performances, sports days, assemblies or celebrations. The Information Commissioner's Office is clear that data protection law does not prevent parents/carers from taking photographs or videos for their own personal or household use. This means that, in many cases, parents/carers taking images of their own child for a family album or personal memories will not be covered by data protection law.

However, education settings may still set their own expectations about photography and filming at events, particularly where there are safeguarding, child protection, privacy or health and safety considerations. This is because images taken at setting events may also include other children, staff, families or visitors, and not everyone will know who may be vulnerable or who may not want their image shared.

Settings should therefore be clear with parents/carers before and during events about what is and is not permitted. For example, settings may allow parents/carers to take photographs or recordings for personal use, but ask that images or videos containing other children, staff or families are not shared publicly or uploaded to open social media platforms without appropriate permission.

The ICO advises that where photos or videos from a setting event are shared on a private social media account, visible only to friends or family, this is likely to remain personal use. However, sharing images or videos on a public account, or in a way that makes them available to an indefinite number of people, may go beyond personal use. In these situations, parents/carers should consider whether the people shown in the images would reasonably expect them to be used in that way, particularly where children are included.

Settings should take a proportionate approach. In most cases, it will be reasonable to allow families to capture special moments involving their own children, while also reminding the wider community to respect the privacy and safety of others. Where there are particular safeguarding concerns, or where photography may cause distress or increase risk for a child, adult or family, settings may need to place additional restrictions on photography or filming.

It may be helpful to provide written guidance to parents/carers before events and, where appropriate, to make a short announcement at the start. This should explain that images are for personal use only, that families should avoid sharing images of other people's children more widely, and that the setting may intervene if photography or filming creates a safeguarding, privacy or health and safety concern.

Further information for parents/carers is available from the ICO guidance on taking photos in schools.

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

Some settings may have parents/carers, staff members, students or other volunteers who are willing to take photographs or videos at events on behalf of the setting. While this can be helpful, it is important to distinguish between parents/carers taking images for their own personal use and someone taking images in an official or volunteer capacity for the setting.

Where a person is taking photographs or videos on behalf of the setting, this should be treated as official image use. The setting remains responsible for ensuring that images are taken, stored, used and shared safely, lawfully and in line with safeguarding and data protection requirements. The safest approach is for any official photographs or recordings to be taken using setting-approved equipment, accounts and storage systems, rather than personal devices. This helps ensure that images remain under the control of the setting and can be securely stored, reviewed, transferred or deleted where necessary.

If a setting is considering allowing a parent/carer, staff member or volunteer to use their own equipment to take images on behalf of the setting, this should be carefully risk assessed and agreed in advance by leaders. The setting should be clear about the purpose of the images, who

has given consent, where images will be stored, how they will be transferred to the setting, when they will be deleted from the individual's device and who will have access to them.
Volunteers acting on behalf of the setting should be made aware that they are expected to follow the setting's safeguarding, confidentiality, image use, acceptable use and data protection policies. They should not use, copy, store, edit, publish or share images for any other purpose, including on personal social media accounts.

Settings should also consider whether it would be more appropriate to use a professional photographer or setting-employed member of staff, particularly where images will be used for publication, marketing, social media or wider communication. Where external photographers or videographers are used, appropriate agreements should be in place to make clear how images will be handled, stored, used and deleted.

Any concerns about the conduct of a person taking images on behalf of the setting, or about how images have been used or stored, should be reported and managed in line with the setting's safeguarding and data protection procedures.

Can education settings ban or restrict mobile phones and personal devices?

Schools should be aware of the DfE guidance on mobile phones in schools, which states that schools should be mobile phone-free environments by default and that pupil use of mobile phones and similar smart technology should be prohibited throughout the school day, including during lessons, the time between lessons, breaktimes and lunchtime. The guidance also explains that references to mobile phones should include other communication and smart technology which the school has decided to include within its policy, such as devices able to send or receive messages or record audio or video.

Schools will therefore need to ensure that their behaviour, mobile phone, online safety and safeguarding policies reflect this national guidance and clearly explain how pupil use of mobile phones and smart technology will be restricted, managed and enforced. Policies should also recognise that some pupils may require reasonable adjustments or agreed exceptions, for example where a device is needed for medical reasons, special educational needs and/or disabilities or caring responsibilities. DfE has identified these as examples of circumstances where some children may need access to mobile phones.

Other education settings, including early years settings, further education settings, alternative provision, out-of-school settings and other organisations working with children and young people, should consider how these safeguarding principles apply within their own context. The DfE "mobile phones in schools" guidance is not written for every type of education setting, so leaders and managers should ensure that their own policies are proportionate, realistic and appropriate to the age, needs and vulnerabilities of the children and young people they work with.

For staff, volunteers, visitors and parents/carers, settings should set clear expectations based on safeguarding, professional conduct, confidentiality, health and safety and operational needs. This may include restricting where and when personal devices can be used, prohibiting the use of personal devices to take photographs or recordings of children, and requiring visitors or volunteers to follow the setting's image use, confidentiality and acceptable use expectations.

A complete prohibition on all adults bringing mobile phones or personal devices onto site may not be practical or necessary in every setting, particularly where staff, visitors or volunteers may need devices for legitimate reasons. However, this does not mean personal devices can be used freely. Settings should be clear that personal phones, cameras, smart watches or other devices must not be used in ways which compromise safeguarding, privacy, professional boundaries or data protection.

Leaders should ensure that expectations are clearly communicated and consistently applied. This may include information for children and young people, parents/carers, staff, volunteers and visitors; appropriate signage; staff induction and regular training; acceptable use agreements; and clear procedures for reporting concerns or responding to breaches. Policies should make clear what is permitted, what is not permitted, and what action may be taken if expectations are not followed.

It is important that staff understand the reasons behind the policy, rather than seeing it as an arbitrary rule. Personal devices and private communication channels can create safeguarding, professional boundary and data protection risks for both children and adults. Leaders should therefore ensure that staff understand how appropriate device use protects children, families, staff and the wider setting community.

Particular care should be taken in early years and other settings where intimate care, changing, toileting, sleeping areas, one-to-one support, transport, trips or close physical care may increase safeguarding sensitivities. In these contexts, leaders should ensure that expectations around personal devices are especially clear, practical and well understood.

DSLs, DPOs, leaders and managers should keep policies under review and ensure that expectations are embedded through safeguarding culture, leadership oversight and regular staff training. Template policies regarding mobile and smart technology, including phones and other personal devices, are available via the LADO Education Safeguarding Advisory Service.

Do we have to pay a fee to the ICO?

Most organisations that process personal information are data controllers and must comply with data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This includes education settings that collect, store or use personal information about children, parents/carers, staff, volunteers or other members of their community.

Data controllers may need to pay a data protection fee to the ICO, unless an exemption applies. The amount payable depends on the organisation's circumstances, including staff numbers, annual turnover and whether the organisation is a public authority, charity or small occupational pension scheme. The ICO currently sets out three fee tiers, with fees ranging from £52 to £3,763.

Some organisations may be exempt from paying the fee, but exemption from the fee does not mean exemption from data protection responsibilities. Settings must still ensure that personal information, including images, is handled lawfully, fairly, securely and transparently.

Education settings should check the ICO's current guidance or use the ICO's self-assessment tool to confirm whether they need to pay a fee and, if so, which tier applies. Further information is available from the ICO's guidance on the data protection fee.

What if something goes wrong?

If an image is lost, shared in error, published without appropriate consent, accessed by someone who should not have seen it, or misused in some way, settings should treat this seriously and respond promptly. Depending on the circumstances, this may be a safeguarding concern, a data protection concern, or both.

Settings should have clear procedures in place so that staff know how to report concerns involving images, including accidental sharing, inappropriate publication, unauthorised access, misuse of images, or concerns that images have been copied, altered or shared more widely than intended. Concerns should be reported to the appropriate senior member of staff, such as the DSL, DPO, headteacher, manager or proprietor.

The setting should consider what immediate action is needed to reduce risk. This may include removing images from websites or social media, asking others to delete or remove content, restricting further access, securing relevant records, supporting any children, families or staff affected, and seeking advice where required.

Where personal data has been affected, settings should assess whether a personal data breach has occurred. The ICO defines a personal data breach broadly and makes clear that organisations should have procedures for detecting, investigating and reporting breaches. The ICO also states that certain personal data breaches must be reported to the ICO within 72 hours of becoming aware of them, where feasible, and that affected individuals must be informed without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

Not every incident will need to be reported to the ICO, but settings should record what happened, what assessment was made, what action was taken and why. The ICO guidance states that organisations must keep a record of personal data breaches, regardless of whether they are required to notify the ICO. Records should be factual, proportionate and limited to the information needed to manage the safeguarding, data protection or conduct concern.

Where there are safeguarding concerns, settings should follow their child protection and safeguarding procedures and consider whether advice or referral to relevant agencies is required. If the concern involves possible criminal activity, blackmail, extortion, harassment, sexual abuse or exploitation, settings should seek appropriate safeguarding and/or police advice.

The ICO has a range of regulatory powers where organisations fail to comply with data protection law. However, the priority for settings should be to act quickly, protect those affected, preserve relevant information, seek appropriate advice and review whether changes are needed to policy, practice, training or systems.

Further guidance is available from the ICO on personal data breaches.

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

Concerns about the use of images, cameras, mobile phones or personal devices should always be taken seriously. This may include concerns about images being taken, stored, shared or published inappropriately; personal devices being used outside agreed procedures; images being accessed by people who do not need to see them; or practice which does not appear to follow the setting's safeguarding, data protection or image use policies.

Where staff, volunteers, parents/carers or children are concerned about image use practice, they should report this through the setting's usual safeguarding and/or data protection procedures. In most cases, this will involve speaking to the DSL, DPO, headteacher, manager or proprietor, depending on the nature of the concern.

If the concern relates to the conduct of a member of staff, volunteer, visitor or another adult working with children, this should be managed in line with the setting's safeguarding and allegations procedures. Where appropriate, advice should be sought from the Local Authority Designated Officer (LADO), children's social care, the police, the ICO or other relevant professionals.

Staff and volunteers should also be aware of the setting's whistleblowing procedures. If they believe unsafe or inappropriate practice is not being addressed, or if they feel unable to raise the concern through normal reporting routes, they should follow the setting's whistleblowing policy. Whistleblowing arrangements should be clearly communicated so that all staff and volunteers know how to raise concerns about poor or unsafe practice, including concerns relating to image use, mobile devices, online safety, professional boundaries or safeguarding culture.

Settings should ensure that concerns are recorded, reviewed and responded to appropriately. This may include taking immediate action to protect children, families or staff; removing or restricting access to images; reviewing whether a data protection breach has occurred; seeking external advice; and considering whether changes are needed to policy, training, supervision or wider safeguarding practice.

If education settings are unsure about their responsibilities in relation to image use, data protection or safeguarding, they should seek advice from appropriate sources. This may include their Data Protection Officer, commissioned data protection or HR services, the ICO, the local authority, safeguarding partners or other relevant professional advisers.

The following links may also be useful to explore recommended national guidance and practice regarding data protection and information sharing:

- Working together to safeguard children - GOV.UK
- Information sharing advice for safeguarding practitioners - GOV.UK
- Data sharing | ICO
- For organisations | ICO
- Data protection in schools - Guidance - GOV.UK

Supporting Guidance

The following information has been provided to support education settings to make informed, safeguarding-led decisions about the taking, use, storage and sharing of images and videos.

This guidance is for general support only and does not constitute legal advice. Settings remain responsible for ensuring that their own policies, procedures and decisions are appropriate for their context and comply with current legislation, statutory guidance and any relevant local or organisational requirements. Where settings are unsure, they should seek advice from an appropriate professional, such as their Data Protection Officer, legal adviser, commissioned data protection service, local authority or other relevant specialist support.

Schools and colleges may also wish to access the DfE Data protection in schools guidance to support wider data protection compliance.

Legislation and consent

Images of identifiable children, young people, staff or other individuals are personal data. Education settings must therefore ensure that photographs and videos are handled in line with data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This applies to images taken, stored, used or shared by the setting for official purposes, including publicity, publications, websites, social media, media activity, learning records, internal systems or wider communication.

Where images are used for publicity, marketing, publication, websites, social media, media activity or other external communications, settings should usually obtain explicit written consent from parents/carers and, where appropriate, involve children and young people in those decisions. Consent should be specific, informed and clearly recorded, so that settings can evidence what has been agreed and for what purpose.

As children mature, settings should take account of their views in an age-appropriate way. Children and young people should be helped to understand how their images may be used, particularly where images may be shared online or more widely. If a child does not want their image to be used, settings should take this seriously, even where parental/carer consent has been given.

Some settings obtain consent on admission, some renew it annually, and others seek consent for specific events, projects or types of use. Whichever approach is taken, settings should ensure that consent arrangements are kept under review and that any changes are recorded promptly. This is particularly important where family circumstances, safeguarding concerns or privacy needs change during a child's time at the setting.

Settings should take particular care where children may be more vulnerable if identified, including children in care, adopted children, children subject to safeguarding plans or court orders, and children or families where there are concerns relating to domestic abuse, stalking, harassment or

other safety risks. In some circumstances, it may be appropriate to seek advice from the DSL, DPO, social worker or other relevant professional before images are taken or used.
Parents/carers have the right to refuse, restrict or withdraw consent for image use. Consent may also be partial, for example allowing some types of image use but not others, such as printed publications but not public websites or social media.

Settings should have clear processes for recording consent, checking it before images are used, and responding promptly if consent is withdrawn or changed. Where people with parental responsibility disagree about image use, settings should take a cautious approach and avoid using the image for the disputed purpose.

Images of children, young people or staff who have left the setting should not normally continue to be used unless there is a clear reason to do so and appropriate consent, or another lawful basis, remains in place. Images that are no longer needed should be securely deleted or destroyed in line with the setting's retention and data protection procedures.

Where consent has not been obtained for publicity, publication or wider sharing, images should not be used for those purposes. If there is disagreement between those with parental responsibility, or uncertainty about who can provide consent, settings should take a cautious approach and seek advice where needed. Where parents/carers consent but the child objects, settings should consider the child's wishes and feelings carefully and avoid using the image unless there is a clear and justified reason to do so.

Settings should carry out regular, documented reviews of images used on websites, social media, displays, newsletters, prospectuses and other promotional materials. This should include checking whether images remain necessary, whether consent remains valid, whether children or staff have left the setting, whether the image remains appropriate in light of current safeguarding information, and whether safer alternatives could now be used.

Not all image use will rely on consent. Where images are used for necessary internal educational, safeguarding, security or administrative purposes, settings should identify and document an appropriate lawful basis under UK GDPR. In these circumstances, settings should ensure that image use is necessary, proportionate, secure, transparent and limited to what is required.

Settings should seek advice from their DPO, commissioned data protection service or other relevant professionals where there is uncertainty about consent, parental responsibility, lawful basis, retention or the safest approach to image use.

AI-enabled image manipulation and abuse

Education settings should ensure that emerging risks linked to artificial intelligence and image manipulation are reflected within image use, safeguarding, online safety, data protection and mobile/smart technology policies.

The UK Council for Internet Safety (UKCIS) Online Harms Early Warning Working Group Protecting your setting's images from AI manipulation and abuse guidance highlights the importance of responsible management, sharing and protection of photographs and videos of children and young people across education settings' websites, social media platforms and other digital spaces. The guidance identifies practical steps settings can consider, including reducing identifiable information, using images that are harder to misuse, applying privacy settings, removing metadata and embedding image security awareness within staff training and policies.

Settings should review existing image use practice and consider whether current arrangements remain appropriate. This should include reviewing images already available on websites, social media channels, prospectuses and other public-facing materials, as well as considering how future images will be selected, approved, published and removed.

Leaders should ensure that staff understand that image security is now part of wider safeguarding and online safety practice. Staff involved in taking, selecting, uploading or approving images should understand the risks of public image sharing, the importance of limiting identifying information, and the need to follow agreed procedures.

When publishing or sharing images, settings should consider whether safer alternatives could be used, such as images of activities, displays or work; group images taken from a distance; over-the-shoulder images; or restricted access platforms rather than public websites or social media. Settings should also ensure they have clear processes for responding if images are misused, altered, copied, shared without consent or used as part of harassment, blackmail, exploitation or other safeguarding concerns. This should include reporting routes, support for affected children, families or staff, and advice from safeguarding, data protection or police professionals where appropriate.

Planning images of children

Still and moving images can bring publications, displays and online communications to life. They can help settings celebrate achievements, share learning and show the wider life of the setting. However, the safety, privacy and dignity of children, staff and families should always be central to decisions about taking and using images.

Before taking or publishing images, settings should consider whether an image of a child or young person is necessary for the intended purpose. In many cases, the same aim may be achieved using less identifiable images, such as photographs of learning activities, displays, children's work, group activities from a distance, over-the-shoulder images, hands-on activities or images where children's faces are not clearly visible.

Settings should avoid routinely using close-up or “passport style” photographs of individual children where a less identifiable image would be suitable. Published images should not normally be accompanied by children’s full names, and settings should avoid including unnecessary identifying information such as uniforms, precise locations, routines or other details which could identify a child, family or member of staff.

Images should always be selected carefully. Children should be appropriately dressed, and particular care should be taken when images are captured during PE, swimming, changing, intimate care or other activities where privacy and dignity may be more sensitive. The taking of images in one-to-one situations with an adult should be avoided unless there is a clear, agreed and necessary reason for doing so. Such situations can be open to misunderstanding and may place both the child and adult in a vulnerable position.

Settings should also consider whether any children, families or staff may be at increased risk if identified. This may include, for example, children in care, adopted children, children subject to safeguarding plans or court orders, families experiencing domestic abuse, or staff or families experiencing harassment, stalking or intimidation. Settings may not always be aware of every circumstance which increases risk, so a cautious and safeguarding-led approach should be taken.

Where images are taken during off-site activities, trips, residential visits or events, settings should ensure the same standards apply. Staff should be clear about which devices may be used, how images will be stored, whether children are allowed to take their own photographs or recordings, and how any images will be reviewed before being shared.

Settings should also consider how images reflect the diversity of their community in a positive, respectful and inclusive way. This should include ensuring children and adults are represented with dignity and avoiding images which could reinforce stereotypes, single out individuals unnecessarily or place anyone at increased risk.

Before publishing or sharing images, settings should ask whether the image is necessary, whether individuals are identifiable, whether consent or another lawful basis applies, whether public sharing is proportionate, and whether a safer alternative would achieve the same purpose. Images should also be reviewed for unnecessary identifying information, metadata, resolution and suitability before publication, and settings should be clear when images will be reviewed or removed.

Online publication of images

When deciding whether to publish or share images online, settings should take a safeguarding-first and risk-based approach. Public image sharing should not be treated as routine; leaders should consider whether it is necessary, proportionate and the safest available option.

Before publishing an image, settings should consider whether the same purpose could be achieved using a less identifiable image or a more restricted method of sharing. For example, images of children's work, displays, activities, group work from a distance or over-the-shoulder images may often be safer than close-up images of individual children. Settings should avoid including unnecessary identifying information alongside images. This includes names, uniforms, precise locations, routines, year groups, class names, achievements or other details which could make it easier for a child, family or member of staff to be identified or located. Particular care should be taken where children, families or staff may be more vulnerable if identified.

Where images are shared online, settings should consider practical steps to reduce the risk of images being copied, altered or misused. This may include removing metadata, using lower-resolution images where appropriate, reviewing privacy settings, limiting downloads where possible, restricting access to known audiences, and using password-protected or closed platforms rather than public websites or social media where this would meet the same purpose more safely. These are all practical image security measures reflected in the UKCIS guidance on protecting settings' images from AI manipulation and abuse.

Settings should recognise that these measures cannot remove all risk once images are shared online. However, they can reduce the likelihood or impact of misuse and support a more thoughtful, safeguarding-led approach to publication.

Image publication decisions should be regularly reviewed by appropriate leaders, including the DSL and DPO where relevant. Reviews should consider whether images remain necessary, whether consent or another lawful basis still applies, whether individuals have left the setting, whether the image remains appropriate in light of any safeguarding information, and whether it should now be removed or replaced.

Checking images before publication

Before images or videos are published or shared publicly, settings should ensure they have been checked carefully for suitability. This is particularly important where images include child(ren), staff, families or visitors and may be shared on websites, social media, newsletters, prospectuses or other public-facing materials.

Where possible, images and videos should be reviewed by ideally at least two appropriate members of staff before publication to help reduce the risk of unsuitable images being published accidentally. This check should consider whether:

- the image is suitable for the intended audience and purpose.
- all child(ren) featured, including any in the background of images, are appropriately dressed.
- the image includes any sensitive, inappropriate or unnecessary identifying information.
- consent or another appropriate lawful basis has been checked.
- the image could increase risk for any child, family member or member of staff.
- a less identifiable image or more restricted sharing method would be safer.

Where there is any uncertainty about whether an image or video is suitable for publication, it should not be shared until advice has been sought from the DSL, DPO or relevant senior leader.

Settings should decide who is authorised to carry out publication checks, for example senior leaders, DSLs, DPOs, communications leads or other appropriate staff. The process should be realistic, consistently followed and recorded where appropriate.

Identifying children in images online

Education settings should use the minimum amount of identifying information when publishing or sharing images of children and young people.

As a general recommendation, settings should avoid publishing a child's full name alongside their image. A simple and safer approach is; **If a child is pictured, do not name them. If a child is named, do not include their image.**

Where an image is used, captions should usually be general and non-identifying, for example "children taking part in outdoor learning" or "pupils working together in science", rather than naming individual children or giving detailed personal information.

If a setting believes there is a clear reason to name a child and use their image, this should be considered carefully, supported by specific consent and assessed in light of any safeguarding, privacy or online safety risks. This is particularly important where images are published online, shared through social media, used in publicity materials or provided to the media.

Settings should also consider whether other information could identify a child, even where their name is not used. This may include the setting name, uniform, year group, class, location, routines, achievements, family details or other contextual information. The more information that is published alongside an image, the easier it may be for a child, family or member of staff to be identified or located.

Where images are shared online, settings should consider whether the same purpose could be achieved using less identifiable information. For example, a general caption such as "group work in science" is likely to be safer than identifying a child by name, class, achievement or personal circumstance.

Particular care should be taken before publishing images or information about children who may be more vulnerable if identified, including children in care, adopted children, children subject to safeguarding plans or court orders, and children or families where there are concerns relating to domestic abuse, stalking, harassment or other safety risks.

Where settings are unsure whether an image or accompanying information could create a safeguarding or privacy risk, they should seek advice from the DSL, DPO or relevant senior leader before publication.

Use of images by parents/carers

Parents and carers often want to take photographs or videos of their own children at setting events, such as performances, sports days, assemblies or celebrations. The Information Commissioner's Office is clear that data protection law does not prevent parents/carers from taking photographs or videos for their own personal or household use. However, settings may still set their own expectations about photography and filming at events where there are safeguarding, child protection, privacy or health and safety considerations.

Where parents/carers are permitted to take photographs or recordings, settings should make expectations clear in advance and, where appropriate, at the start of the event. This should include reminding families that images are for personal use and asking them to think carefully before sharing images or recordings more widely, particularly where other children, staff, families or visitors may be included.

The ICO advises that sharing photos or videos from a school event on a private social media account, visible only to friends or family, is likely to fall within personal use. However, sharing images on a public account, or in a way that makes them available to an indefinite number of people, is likely to go beyond personal use. In those circumstances, parents/carers should consider whether the individuals in the images would reasonably expect them to be used in that way, especially where children are included.

Settings should take a proportionate approach. In most cases, it will be reasonable to allow families to capture special moments involving their own children, while also reminding the community to respect the privacy and safety of others. However, settings may decide to restrict or refuse photography or filming where there are particular safeguarding concerns, where children or adults may be placed at risk, or where photography creates health and safety issues, for example through excessive use of flash, bulky equipment or obstruction of others.

Settings should also remain alert to individuals who have no clear connection to the setting or event and who may be attempting to take photographs or recordings without permission. Staff should know how to respond safely and in line with the setting's safeguarding procedures if they are concerned about anyone filming or photographing children or adults.

This advice applies to parents/carers taking images for their own personal use. A different position applies where a parent/carer, volunteer or other individual is taking photographs or videos on behalf of the setting. In those circumstances, the individual is acting in an official or volunteer capacity and must follow the setting's safeguarding, confidentiality, image use, acceptable use and data protection procedures.

Use of images by children

Many education settings use cameras, tablets or other devices with imaging capabilities as part of learning. Children may use images and videos to record activities, document learning, reflect on their work or develop digital skills. This can be a positive and creative part of education when it is well supervised and supported by clear expectations.

Where children are taking photographs or videos as part of setting-led activities, staff should ensure that this takes place in a safe, respectful and appropriately supervised environment. Children should be taught, in an age-appropriate way, that they should ask permission before taking images of others and that everyone has the right to say no to being photographed or recorded.

Settings should agree clear boundaries for children's use of cameras and devices. This should include where devices may and may not be used, how images will be checked, where they will be stored and whether they will be shared with parents/carers or displayed within the setting. Devices should not be used in sensitive areas such as toilets, changing areas, sleeping areas or other spaces where privacy and dignity could be compromised.

Staff should be aware that children may unintentionally or deliberately take images which are inappropriate, intrusive or harmful. This may include images which compromise another child's privacy or dignity, are taken without consent, or are shared beyond the intended context. Such incidents should be managed in line with the setting's safeguarding, behaviour, online safety and data protection procedures.

Where children are taking images for official use by the setting, this should be treated as setting-controlled image use. Parents/carers should be informed that children may take photographs or videos as part of learning activities, how these images will be managed, and whether they will be used internally only or shared more widely. Consent arrangements should be followed, particularly where images include other children.

Images taken by children as part of setting-led activity should be carefully reviewed before being displayed, shared with parents/carers, uploaded to online systems or shown on digital screens. Settings should take particular care where images include children who may be more vulnerable if identified, such as children in care, adopted children, children subject to safeguarding plans or court orders, or children and families where there are known safety concerns.

Where children are allowed to bring or use personal devices, settings should ensure this is addressed within their mobile and smart technology policy and Acceptable Use Policy. Expectations should be clear for children, staff and parents/carers, including when devices may be used, where they must be stored, what image-taking is not permitted, and what action may be taken if devices or images are misused.

Residential visits, trips, changing areas, swimming activities and overnight stays require particular care. Settings should ensure that children understand safe and respectful use of devices in these contexts and that staff supervision arrangements are clear.

Storage of images

Images should be stored securely, even where they are only being kept for a short period of time. Education settings should ensure that photographs and videos are stored on approved setting systems, with appropriate access controls in place. Access should be limited to staff who need the images for a legitimate professional purpose.

Images should not be stored on personal devices, personal cloud accounts, personal email accounts or personal messaging apps. Where setting-provided devices are used to take images, images should be transferred to an approved secure system as soon as possible and deleted from the original device once this has been done, unless there is a clear reason for temporary retention.

Portable storage devices should only be used where this has been authorised and where appropriate security measures are in place, such as encryption, password protection and clear logging arrangements. Images should not be retained on portable devices for longer than necessary.

Where settings use apps, learning platforms, cloud storage, social media tools or third-party systems to store or share images, leaders should ensure that these have been appropriately risk assessed before use. This should include consideration of where images are stored, who can access them, how long they are retained, how they can be deleted, and whether the provider's terms and conditions allow images to be reused, shared or processed in ways the setting would not expect.

Settings should ensure that any use of third-party platforms or systems complies with data protection legislation and the setting's own safeguarding, online safety, image use and data protection policies. A DPIA should be considered where a system or process is likely to involve higher risk, particularly where images of children are being stored, shared or accessed through online platforms.

Images should not be kept indefinitely. Settings should have clear arrangements for reviewing, retaining and deleting images, including images held on websites, social media channels, apps, displays, newsletters, prospectuses, cloud storage and archived folders. Images should be securely deleted or destroyed when they are no longer needed, when consent no longer applies, or when continued retention would no longer be necessary or proportionate.

Staff should receive clear guidance on where images must be stored, who may access them, how they should be transferred, and how and when they should be deleted. This should form part of wider safeguarding, data protection and online safety training.

Use of images of children by the press/media

There may be occasions when members of the press or media are invited to a planned event to photograph, film or interview children, for example to celebrate achievements, community events, performances or fundraising activities. While this can be positive for the setting and its community, leaders should consider carefully how press or media involvement will be managed before access is agreed.

Images taken by the press or media may be published more widely than setting-controlled images, including online, in print and through social media channels. Once published, the setting may have limited control over how images are shared, copied or reused. Settings should therefore ensure that parents/carers, and children where appropriate, understand how press or media images may be used before consent is sought.

The setting should obtain appropriate consent before children are photographed, filmed or interviewed by the press or media. Where a parent/carer does not give consent, or where a child does not wish to be involved, this must be respected. Particular care should be taken where children, families or staff may be more vulnerable if identified, including children in care, adopted children, children subject to safeguarding plans or court orders, or families affected by domestic abuse, stalking, harassment or other safety concerns.

Press and media organisations may process personal information for journalistic purposes, and data protection law includes exemptions in some circumstances for journalism. However, this does not remove the setting's responsibility to manage access to children safely, check consent, consider safeguarding risks and communicate clearly with families. The ICO states that exemptions should not be relied on routinely and should be considered case by case.

Where press or media attendance is planned, settings should agree expectations in advance. This may include confirming who will attend, checking identification on arrival, agreeing which children may be photographed or interviewed, limiting detailed captions, avoiding full names where possible, and ensuring staff are available to supervise media activity. Particular care should be taken with one-to-one interviews, close-up images, sports or performance photography, and any situation where children may be identifiable in a sensitive context.

Settings should also be aware that press and media organisations may be subject to relevant editorial codes and industry standards. IPSO guidance states that children are given a higher level of protection than adults under the Editors' Code, and that consideration should be given to who can consent for publication of material involving a child's private life or welfare and how that consent is documented.

If the setting is unsure whether media access is appropriate, or whether particular children should be included, advice should be sought from the DSL, DPO, senior leadership team or relevant local authority/commissioned adviser before the event.

Use of external photographers/videographers

Education settings may choose to engage external photographers or videographers for events, individual or group photographs, promotional materials, performances, celebrations or other agreed purposes. Where this happens, leaders should ensure that photographers and videographers understand and agree to follow the setting's safeguarding, image use, confidentiality and data protection expectations.

Where an external photographer or videographer is processing images on behalf of the setting, the setting will usually remain responsible for deciding why and how the images are used. In these circumstances, the photographer or videographer is likely to be acting as a data processor, and a written contract or agreement should be in place. The ICO states that whenever a controller uses a processor, there must be a written contract or other legal act in place so that both parties understand their responsibilities and liabilities.

The agreement should make clear the purpose of the photography or filming, what images may be taken, how they will be stored, who may access them, how long they will be retained and how they will be securely deleted or returned to the setting. It should also make clear that images must not be used for any other purpose, shared with third parties, uploaded to personal or unauthorised platforms, or used in the photographer's own publicity unless this has been specifically agreed and appropriate consent is in place.

Settings should satisfy themselves that any external photographer or videographer can handle images safely and securely. This should include considering their approach to confidentiality, secure storage, transfer of images, deletion arrangements, use of assistants or sub-contractors, and whether any online galleries or ordering systems are used. Where online systems are used, settings should understand who can access the images, how access is controlled, how long images remain available and whether the provider's terms and conditions allow any onward use.

Relevant checks should be completed before the event or activity. This may include confirming the photographer or videographer's identity, checking the organisation or individual is reputable, agreeing supervision arrangements, and considering whether any suitability checks are required depending on the nature of the activity and level of contact with children. Photographers and videographers should not have unsupervised access to children unless this has been appropriately considered and authorised in line with the setting's safeguarding procedures.

On arrival, the identity of the photographer or videographer should be checked, and staff should know who has been authorised to take images. If there are concerns about the authenticity, conduct or behaviour of a photographer or videographer, access should be refused or withdrawn, and the concern should be reported in line with the setting's safeguarding procedures.

Where staff, parents/carers or volunteers take photographs or videos on behalf of the setting, they should be treated as acting in an official capacity and should follow the same safeguarding, confidentiality, image use and data protection expectations. The safest approach is for official images to be taken, stored and transferred using setting-approved equipment, accounts and systems.

Use of video surveillance, including closed-circuit television (CCTV)

Any use of video surveillance, including CCTV, webcams used for surveillance purposes, doorbell-style cameras, body-worn cameras or other recording technologies, should be considered carefully and managed in line with data protection legislation and relevant Information Commissioner's Office (ICO) guidance. The ICO provides guidance to help organisations consider installation, management, operation, public awareness and signage.

Video surveillance may be used for a range of legitimate purposes, such as site security, controlling access, deterring or detecting crime, supporting health and safety, managing premises and investigating incidents or concerns. In some settings, leaders may also consider whether surveillance supports wider safeguarding or safer working arrangements. However, surveillance should only be used where it is necessary, proportionate and justified for a clearly defined purpose.

Settings should not assume that CCTV is automatically the best or only solution. Before installing or continuing to use video surveillance, leaders should consider the benefits, limitations and possible impact on children, families, staff and visitors. This should include considering whether the same aim could be achieved through less intrusive measures, such as improved supervision, staffing arrangements, site management, access controls, safer working practice, whistleblowing arrangements or clearer behaviour expectations.

Settings should identify and document an appropriate lawful basis for using video surveillance and should consider whether a DPIA is required. This will be particularly important where surveillance may capture children, staff or visitors in ways that could affect privacy, dignity or trust, or where cameras are used in sensitive areas of the setting.

Individuals should be clearly informed that video surveillance is in use before they enter monitored areas. Signage and privacy information should explain why recording is taking place, who is responsible for the system, how recordings may be used, who may access them and how long they will be retained. The purpose of surveillance should be communicated clearly to the setting community, for example whether it is used for security, health and safety, safeguarding or site management.

Cameras should be positioned carefully and sensitively. They should not be placed in areas where individuals have a high expectation of privacy, such as toilet cubicles, changing areas or intimate care spaces. Particular care should be taken where cameras are near toilets, changing rooms, sleeping areas or other sensitive parts of the setting, to ensure privacy and dignity are protected.

Recordings should be stored securely, accessed only by authorised individuals and retained only for as long as necessary. Settings should ensure that manufacturer guidance, privacy settings, access controls and data protection requirements are understood and followed. Arrangements should also be in place for responding to requests to access footage, sharing recordings with other agencies where appropriate, and securely deleting recordings when they are no longer required.

The continued use of video surveillance should be reviewed regularly. Reviews should consider whether the system remains necessary and proportionate, whether cameras are positioned appropriately, whether signage and privacy information remain accurate, whether access to footage is properly controlled, and whether surveillance is supporting, rather than replacing, strong safeguarding, supervision and safer working practice.

Further advice is available from the ICO guidance on CCTV and video surveillance.

Use of webcams

Some education settings may use webcams or similar video technology for different purposes, including remote learning, curriculum activities, communication with families, site security or surveillance. Settings should be clear about the purpose of any webcam use, who will be able to access the images or recordings, whether sessions will be recorded, and how any images, video or audio will be stored and protected.

Where webcams are used for surveillance or security purposes, they should be treated in the same way as other forms of video surveillance. Settings should ensure that use is necessary, proportionate and justified, and that individuals are clearly informed before entering areas where recording takes place. Signage and privacy information should explain why recording is taking place, who is responsible for the system, how recordings may be used, who may access them and how long they will be retained. The ICO provides guidance on CCTV and video surveillance, including the use of video surveillance technologies and a self-assessment checklist for organisations.

Where webcams are used for curriculum purposes, online learning, meetings or communication, settings should consider safeguarding, privacy and data protection risks before use. Children, parents/carers and staff should be given clear information about why webcams are being used, whether cameras are expected to be switched on, whether sessions will be recorded, how images or recordings will be used, and what expectations apply to screenshots, private recordings or onward sharing.

If webcam use involves recording identifiable children, young people, staff or families, settings should identify an appropriate lawful basis and ensure that any consent arrangements are clear where consent is being relied upon. In some circumstances, it may be more appropriate to use alternatives such as audio only, blurred backgrounds, initials rather than full names, pre-recorded content, or activities which do not require children or staff to be visible on camera.

Recordings should only be made where there is a clear and justified purpose. They should be stored securely, accessed only by authorised individuals and retained only for as long as necessary. Settings should also ensure that any platform or system used for webcam activity has been appropriately risk assessed and is used in line with the setting's safeguarding, online safety, image use and data protection policies.

Particular care should be taken where webcams may capture private home environments, vulnerable children or families, one-to-one work, intimate care areas, sleeping areas, changing areas or any other context where privacy and dignity may be more sensitive. Staff should receive clear guidance on safe and appropriate webcam use, including the use of setting-approved devices, accounts and platforms.

Copyright

Education settings should be aware that copyright may apply to photographs, videos, illustrations and other images they use, including images found online. Images should not be copied, downloaded, adapted, uploaded to websites, included in newsletters or used on social media unless the setting has permission, a suitable licence, or another lawful basis for using them.

Photographs, illustrations and other images are generally protected by copyright as artistic works. The copyright owner has rights over how the work is copied, adapted, issued, communicated or shared, including online. The creator of an image is usually the first copyright owner, although there are exceptions, such as where an image is created by an employee as part of their employment.

Settings should not assume that images found through internet searches, websites, social media or image libraries are free to use. Before using an image from another source, settings should check the licence terms carefully, including whether the image can be used for education, publicity, websites, social media, printed materials or commercial/promotional purposes. Any required credit or attribution should be included.

Commissioning or paying for photographs, video or design work does not automatically mean the setting owns the copyright. Where settings use professional photographers, videographers, designers or freelancers, contracts should make clear who owns the copyright, what the setting is allowed to do with the images or recordings, whether they can be edited or reused, and whether the photographer or provider may use them for their own publicity.

State-funded primary and secondary schools in England should also be aware of copyright licences purchased centrally by the Department for Education. These licences cover schools for many copyright requirements, but school leaders remain responsible for ensuring that intended activities are covered and that staff follow the relevant terms and conditions. Other education settings, including early years settings, independent settings, colleges, alternative provision and out-of-school settings, should check what licences or permissions apply to their own organisation.

Settings should also take care when using stock images, Creative Commons images or AI-generated images. Licence terms may vary and may include restrictions on editing, attribution, commercial use or online publication. Where images include identifiable people, settings should also consider privacy, consent and safeguarding implications, even if copyright permission appears to be in place.

It is good practice for settings to keep records of permissions, licences, contracts and attribution requirements for images they use. Where there is uncertainty about whether an image can be used, settings should seek advice before publication or use an alternative image that they are confident they have permission to use.

Further information is available from the Intellectual Property Office guidance on digital images, photographs and the internet, the Department for Education guidance on copyright licences for state schools in England, and the Copyright Licensing Agency.

Public Image Sharing Checklist

This checklist is intended to support proportionate decision making and should be adapted to reflect the setting's own policy, procedures, systems and safeguarding context.

If there is any uncertainty, images should not be published until advice has been sought from the DSL, DPO or relevant senior leader.

Before publishing or sharing images publicly, settings should consider the following:

- ❑ **Is the image necessary?**
  Could the same purpose be achieved without using an image of a child, young person or member of staff?

- ❑ **Is public sharing necessary?**
  Could the image be shared more safely through a restricted platform, parent portal, internal system or direct communication instead?

- ❑ **Could a less identifiable image be used?**
  For example, could the setting use an image of children's work, displays, activities, hands, backs of heads, group work from a distance or an over-the-shoulder image?

- ❑ **Does the image identify anyone directly or indirectly?**
  Consider whether the image or accompanying information includes faces, full names, uniforms, setting name, year group, class, location, routines, timetables, achievements, family details or other contextual information.

- ❑ **If a child is pictured, have names been avoided?**
  As a safer general approach: if a child is pictured, do not name them; if a child is named, do not include their image.

- ❑ **Could the image increase risk for a child, family or member of staff?**
  Consider whether anyone pictured may be at increased risk if identified, for example, children in care, adopted children, children subject to safeguarding plans or court orders, families affected by domestic abuse, or staff/families experiencing harassment, stalking or intimidation. Staff may not know this information so advice should be sought from the DSL, DPO or relevant senior leader.

- ❑ **Has consent been checked and recorded?**
  Check that consent is current, specific to the intended use, and has not been withdrawn or restricted.

- ❑ **Have the child's wishes been considered?**
  Where appropriate, has the child or young person been involved in the decision and are they comfortable with the image being used?

- ❑ **Are there any parental responsibility or consent disagreements?**
  If people with parental responsibility disagree, or the position is unclear, has the setting taken a cautious approach and sought advice where needed?

- ❑ **Has the lawful basis been considered?**
  Where consent is not the basis for image use, has the setting identified and documented an appropriate lawful basis?

- ❑ **Has unnecessary identifying information been removed?**
  Check captions, file names, alt text, tags, hashtags, embedded details and accompanying text.

- ❑ **Has metadata been removed where possible?**
  This may include location, device details, timestamps or other embedded information.

- ❑ **Has the image quality/resolution been considered?**
  Would a lower-resolution image meet the same purpose while reducing risk of misuse?

- ❑ **Is the platform appropriate and secure?**
  Consider privacy settings, audience, download options, sharing controls, platform terms and whether public posting is necessary.

- ❑ **Has the image been approved before publication?**
  Has the image been checked by an appropriate member of staff, such as the DSL, DPO, senior leader or communications lead, depending on the setting's procedure?

- ❑ **Has a suitability check been completed?**
  Before publication, has the image or video been checked by ideally at least two appropriate members of staff to confirm child(ren) are appropriately dressed, the image is suitable for the intended audience, and no sensitive or unnecessary identifying information is visible?

- ❑ **Has the setting recorded where the image has been published?**
  This will support future review, removal and response if consent changes or a concern arises.

- ❑ **When will the image be reviewed or removed?**
  Set a review or removal date, particularly for website, social media, newsletters, prospectuses and promotional materials.

- ❑ **Does the benefit outweigh the safeguarding, privacy and data protection risk?**
  If not, use an alternative image or do not publish.

Sample Image Use Policy Template

[Setting Name] Image Use Policy

[Setting Logo]

Settings should ensure this policy is adapted to reflect their own:

- ***age range and terminology***
- ***setting type and governance arrangements***
- ***lawful bases for different types of image use***
- ***consent recording and checking systems***
- ***communication platforms and social media channels***
- ***CCTV/video surveillance arrangements***
- ***use of parent/carer platforms or learning journals***
- ***retention schedules***
- ***DPO or commissioned data protection support***
- ***safeguarding procedures and local reporting pathways***

The policy should be reviewed regularly and updated in response to changes in legislation, statutory guidance, national advice, technology, local procedures or emerging safeguarding risks.

Key Details

Policy written by: [Name, Role]

Approved by Governing Body on: [DD/MM/YY]

Date to be reviewed: [DD/MM/YY] ***Note: 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 and recordings taken, stored, used or shared by **[school/setting name]** are managed lawfully, safely and appropriately, with due regard to safeguarding, online safety, privacy and data protection.

2. This policy applies to all members of the **[school/setting]** community, including child(ren), parents/carers, staff, **[governors/proprietors],** volunteers, students, visitors, contractors,

external providers and any other individuals who take, use, store, access or share images on behalf of, or within, the **[school/setting]**. ***Amend as appropriate***

3. This policy must be read alongside other relevant policies, including but not limited to child protection, behaviour, anti-bullying, online safety, data protection, privacy notices, staff code of conduct/safer working practice, acceptable use, mobile and smart technology, social media, confidentiality, whistleblowing, low-level concerns/allegations, CCTV/video surveillance and relevant curriculum policies. ***Amend as appropriate***

4. This policy applies to all images and recordings, including still photographs, video recordings, livestreams, webcam images, CCTV/video surveillance footage and any other digital image or recording taken, stored, used or shared by, or on behalf of, **[school/setting name]**. ***Amend as appropriate***

5. Images of identifiable individuals are personal data. **[School/setting name]** will ensure that images are processed in line with data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Images will be processed:
    - fairly, lawfully and in a transparent manner
    - for specified, explicit and legitimate purposes
    - in a way that is adequate, relevant and 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 leadership team, supported by the Data Protection Officer (DPO) **[name, role]**, Designated Safeguarding Lead (DSL) **[name, role]** and **[governing body/proprietor/management committee]**, is responsible for ensuring the safe, lawful and appropriate use, storage, sharing and disposal of images. This includes implementation, monitoring, staff training and regular review of this policy.

Official use of images of children

Consent, lawful basis and transparency

7. Consent will not be treated as a one-off administrative process. **[School/setting name]** will review consent arrangements regularly and at key transition points to ensure parents/carers and, where appropriate, child(ren), understand how images may be used.

8. Child(ren)'s wishes and feelings will be sought and taken into account in an age-appropriate way. Images will not normally be taken or used where a child indicates that they do not wish to be photographed or recorded, unless there is a clear and justified reason to do so.

9. Where images are used for publicity, publication, websites, social media, media activity, marketing or wider external communication, written consent will usually be obtained from

parents/carers, unless another appropriate lawful basis has been identified and documented. Child(ren)'s wishes and feelings will be sought and taken into account where appropriate.

10. Where images are used for necessary internal educational, safeguarding, security or administrative purposes, **[School/setting name]** will identify an appropriate lawful basis and ensure images are used only where necessary, proportionate and secure. Consent may not be the most appropriate lawful basis for these necessary internal uses.

11. Specific consent will be sought where images are used for training, publicity, marketing, media activity, online broadcasts or any purpose not covered by the original consent.

12. Consent records will be retained securely for as long as the relevant image is in use and in line with the **[school/setting's]** data retention arrangements. Any sensitive image-use concerns will be recorded separately and securely, with access limited to staff who need to know in order to safeguard the child or manage image use appropriately.

13. Consent will be requested on **[insert basis, e.g. admission, annually, at key transition points or for specific activities/events]** and reviewed when circumstances change.

14. Where consent is refused, restricted or withdrawn, **[School/setting name]** will update its records promptly and take reasonable steps to stop further use of the relevant images and remove them from **[school/setting]**-controlled platforms where practicable.

15. Where people with parental responsibility disagree about image use, or where the position is unclear, **[School/setting name]** will take a cautious approach and avoid using the image for the disputed purpose until the matter is resolved or appropriate advice has been sought. ***Note: The Department for Education's guidance on parental responsibility for schools states that the welfare of the child must be a school's paramount consideration and that schools should seek legal advice where they are unsure how to act in relation to parental responsibility concerns. Other education settings should take a similarly cautious approach and seek appropriate advice where needed.***

Safety of images

16. **[School/setting name]** recognises that images and videos shared online may be copied, downloaded, scraped, altered, manipulated, redistributed or reused without the **[school/setting's]** knowledge or consent. This includes potential misuse through artificial intelligence and other digital tools.

17. Decisions about taking, storing and publishing images will be made using a safeguarding-first approach, considering whether the image is necessary, proportionate and the least identifiable option available. This may include reducing identifiable information, using images that are harder to misuse, applying privacy settings, removing metadata and embedding image security awareness within staff training and policies.

18. All official images taken or processed by or on behalf of **[School/setting name]** will be taken using school/setting-approved equipment, accounts, platforms and systems wherever possible.

19. Staff will receive information regarding safe and appropriate image use as part of induction and regular safeguarding, online safety and data protection training. This will include consent, lawful basis, storage, publication, online sharing risks, AI-enabled image manipulation, personal devices, and how to recognise and respond to concerns involving image misuse, alteration, non-consensual sharing or threats involving images.

20. Staff will:
    - only take, use or publish images where there is a clear **[school/setting]** purpose and the relevant consent, lawful basis and safeguards have been checked.
    - ensure that a senior member of staff is aware that official images are being taken and for what purpose.
    - take account of the child's wishes and feelings wherever possible and appropriate, particularly where images are used for publication, publicity or wider sharing.
    - avoid taking images in one-to-one situations unless there is a clear, agreed and necessary reason for doing so.
    - report concerns about image use promptly in line with safeguarding, data protection, whistleblowing or other relevant procedures.

21. Staff will not
    - take images of child(ren) for personal use.
    - use personal devices, personal accounts or personal communication channels to take, store or share images of child(ren). ***Note: If headteachers/managers opt to allow staff to use personal equipment to take photos/videos of children, clear boundaries and expectations should be detailed. For example, unless this has been explicitly authorised in exceptional circumstances, risk assessed and managed in line with school/setting procedures. This is essential to safeguard all members of the community.***
    - display, distribute or publish images unless authorised and the relevant consent or lawful basis has been checked.
    - take images of child(ren) in a state of undress or semi-undress, or images which could reasonably be considered inappropriate, indecent or sexual.
    - take photographic, video or audio evidence of child(ren)'s injuries, marks, bruising, disclosures or similar safeguarding concerns. Concerns must be recorded and reported in line with the **[school/setting]** child protection policy and procedures.

22. All members of staff, including volunteers, will ensure official images are available for scrutiny and that they can justify the purpose, storage and use of any official images in their possession.

Storage, retention and review of images

23. Images will only be retained when there is a clear and agreed purpose for doing so.

24. Images will be stored securely on approved **[school/setting]** systems, with access limited to authorised staff who need to use them for a legitimate purpose.

25. Images will not be stored on staff personal devices, personal cloud accounts, personal email accounts or personal messaging apps.

26. Where images are temporarily stored on cameras, memory cards, portable devices or other equipment, they will be transferred to an approved secure system as soon as practicable and deleted from the original device unless there is a clear and authorised reason for temporary retention.

27. Portable storage devices will only be used where authorised and where appropriate safeguards are in place, such as encryption, password protection, logging and secure deletion.

28. **[School/setting name]** will carry out regular, documented reviews of images used on websites, social media channels, displays, newsletters, prospectuses, promotional materials, apps and other platforms. Reviews will consider whether images remain necessary, whether consent or another lawful basis still applies, whether individuals have left the setting, whether safeguarding circumstances have changed, and whether images should be removed or replaced. ***Note: Settings should specify how often this review will take place, for example termly, biannually or annually, and who will be responsible for completing and recording it.***

29. Images will be securely deleted, destroyed or archived in line with the school/setting's retention schedule when they are no longer required.

30. The [**Headteacher/Manager]**, DPO and/or DSL may request access to official images and may withdraw or amend a member of staff's authorisation to take, use or share images at any time where concerns arise regarding safeguarding, professional conduct, policy compliance or data protection.

31. Any apps, websites, cloud services, learning platforms or third-party companies used to share, host, print, store or access child(ren)'s images will be risk assessed before use. Where required, a Data Protection Impact Assessment (DPIA) will be completed.

Safe Practice when taking images

32. Careful consideration will be given before involving very young child(ren), child(ren) with additional needs, or child(ren) who may be more vulnerable, particularly where they may be less able to understand or question why images are being taken.

33. **[School/setting name]** will discuss image use with child(ren) in an age-appropriate way and will support them to understand that they have a right to say no to being photographed or recorded wherever possible.
34. Photography or video recording is not permitted in sensitive areas such as toilets, changing areas, intimate care areas, sleeping areas, swimming areas or other locations where privacy and dignity may be compromised.

35. Images or videos that include child(ren) will be selected carefully and will only be used where they are appropriate for the intended purpose.

36. Child(ren) will be appropriately dressed in any images used by the **[school/setting]**. Particular care will be taken when selecting images from PE, swimming, performances, residential visits or other activities where privacy, dignity or context may be more sensitive.

37. Images taken during off-site activities, trips, residential visits or events will be managed in line with this policy. Staff will be clear about which devices may be used, how images will be stored, whether child(ren) may take their own photographs or recordings, and how images will be reviewed before any sharing takes place.

Publication and sharing of images

38. When selecting images for publication or sharing, **[School/setting name]** will consider whether the image is necessary, proportionate and appropriate for the intended purpose.

39. Where possible, **[School/setting name]** will use images that reduce identifiability, such as group images taken from a distance, over-the-shoulder images, images of work or activities, displays, or images where child(ren)'s faces are not clearly visible.

40. Where images are published online, **[School/setting name]** will avoid using full names or unnecessary identifying information. In most cases, child(ren) who are pictured will not be named. If there is a clear reason to use a child's full name alongside their image, specific consent will be sought first.

41. **[School/setting name]** will not include personal addresses, personal email addresses, telephone numbers or other unnecessary contact information in images, captions, videos, websites, prospectuses or other publications.

42. Where images are shared online, **[School/setting name]** will consider whether public sharing is necessary or whether a more restricted method of sharing can be used. Where appropriate, privacy settings, closed platforms, password-protected areas or limited-access groups will be used to reduce the visibility and onward sharing of child(ren)'s and staff images

43. Where appropriate and proportionate, **[School/setting name]** will consider practical measures to reduce the risk of images being copied, altered or misused. This may include removing metadata, using lower-resolution images, applying watermarking, limiting downloads where possible, reviewing privacy or access settings, and regularly removing images that are no longer needed. These measures cannot remove all risk but may help reduce the likelihood or impact of misuse.

44. Before any image or video of child(ren) is published or shared publicly, it should be checked by **[at least two]** appropriate members of staff to ensure it is suitable, proportionate and does not include inappropriate, sensitive or unnecessary identifying information. This should include checking that child(ren) are appropriately dressed and that consent/lawful basis has been considered. Where there is any uncertainty, the image should not be published until advice has been sought from the DSL, DPO or relevant senior leader. ***Adapt according to setting decisions and policy/processes***

Use of apps, systems and platforms to share images with parents/carers

Note: Remove this section if the setting does not use apps, online learning journals, parent/carer platforms or similar systems

45. **[School/setting name]** uses **[name of system/platform]** to upload and share images of child(ren) with parents/carers.

46. The use of **[name of system/platform]** has been appropriately risk assessed. Where required, a DPIA has been completed.

47. The **[governing body/headteacher/manager/proprietor]** has taken steps to ensure that data and images stored or shared through the system are handled in accordance with data protection legislation and the **[school/setting]** safeguarding, online safety and image use policies.

48. Images uploaded to **[name of system/platform]** will only be taken on school/setting-approved devices, accounts and systems.

49. Staff, parents/carers and other authorised users will be provided with clear expectations regarding safe and appropriate use before access is given. This will include expectations regarding passwords, access sharing, downloading, copying, screenshotting, onward sharing and reporting concerns.

Use of Video Surveillance, including CCTV

Note: Remove this section if the setting does not use video surveillance

50. Any use of video surveillance, including CCTV, webcams used for surveillance purposes, doorbell-style cameras, body-worn cameras or other recording technologies, will be considered carefully and managed in line with data protection legislation and relevant

Information Commissioner's Office guidance. ***Note: The ICO provides guidance and a CCTV self-assessment checklist to help organisations consider installation, management, operation, public awareness and signage.***

51. Video surveillance will only be used where it is necessary, proportionate and justified for a clearly defined purpose, such as site security, controlling access, deterring or detecting crime, supporting health and safety, managing premises, investigating incidents or supporting wider safeguarding or safer working arrangements.

52. **[School/setting name]** will not assume that CCTV is automatically the best or only solution. Before installing or continuing to use video surveillance, leaders will consider whether the same aim could be achieved through less intrusive measures, such as improved supervision, staffing arrangements, site management, access controls, safer working practice, whistleblowing arrangements or clearer behaviour expectations.

53. **[School/setting name]** will identify and document an appropriate lawful basis for using video surveillance and will consider whether a DPIA is required.

54. Individuals will be clearly informed that video surveillance is in use before entering monitored areas. Signage and privacy information will explain why recording is taking place, who is responsible for the system, how recordings may be used, who may access them and how long they will be retained.

55. Cameras will be positioned carefully and sensitively. They will not be placed in areas where individuals have a high expectation of privacy, such as toilet cubicles, changing areas or intimate care spaces.

56. Particular care will be taken where cameras are near toilets, changing rooms, sleeping areas or other sensitive parts of the setting to ensure privacy and dignity are protected.

57. Recordings will be stored securely, accessed only by authorised individuals and retained only for as long as necessary. The default retention period will be **[insert period, for example 30 days]**, unless there is a clear reason to retain footage for longer, such as an incident, safeguarding concern, complaint or investigation.

58. The continued use of video surveillance will be reviewed regularly. Leadership reviews will consider whether the system remains necessary and proportionate, whether cameras are positioned appropriately, whether signage and privacy information remain accurate, whether access to footage is properly controlled, and whether surveillance is supporting, rather than replacing, strong safeguarding, supervision and safer working practice.

Use of webcams

Note: Remove this section if the setting does not use webcams

59. Webcams or similar video technology may be used for remote learning, curriculum activities, communication with families, site security or surveillance. ***Amend as appropriate***

60. **[School/setting name]** will be clear about the purpose of webcam use, who will be able to access the images or recordings, whether sessions will be recorded, and how images, video or audio will be stored and protected.

61. Where webcams are used for surveillance or security purposes, they will be treated in the same way as other forms of video surveillance.

62. Where webcams are used for curriculum purposes, online learning, meetings or communication, safeguarding, privacy and data protection risks will be considered before use.

63. Child(ren), parents/carers and staff will be given clear information about why webcams are being used, whether cameras are expected to be switched on, whether sessions will be recorded, how images or recordings will be used, and what expectations apply to screenshots, private recordings or onward sharing.

64. Where webcam use involves recording identifiable child(ren), staff or families, **[School/setting name]** will identify an appropriate lawful basis and ensure that consent arrangements are clear where consent is being relied upon.

65. Recordings will only be made where there is a clear and justified purpose. They will be stored securely, accessed only by authorised individuals and retained only for as long as necessary.

66. Particular care will be taken where webcams may capture private and/or home environments, vulnerable child(ren) or families, one-to-one work, intimate care areas, sleeping areas, changing areas or any other context where privacy and dignity may be more sensitive.

Use of images by parents/carers

67. Parents/carers may take photographs or video footage of their own child(ren) at school/setting events for personal and family use, unless advised otherwise by the school/setting. ***Note: The Information Commissioner's Office explains that data protection law does not stop parents/carers taking photos or videos for their own personal or household use. However, schools/settings may set their own expectations for safeguarding, child protection, privacy or health and safety reasons.***

68. Parents/carers are expected to follow any instructions given by staff before, during or after an event regarding photography or filming. The **[school/setting]** may restrict or refuse photography or filming where this is necessary for safeguarding, privacy, dignity, health and safety or operational reasons.

69. Where photographs or videos also include other child(ren), staff, families or visitors, parents/carers are expected not to share these images publicly or upload them to open social media without permission.

70. Parents/carers are not permitted to take photographs or video recordings in sensitive areas of the **[school/setting],** including toilets, changing areas, intimate care areas, swimming areas, sleeping areas or any other area where privacy and dignity may be compromised.

71. Parents/carers are asked not to copy, download, screenshot, redistribute or publicly share images taken or provided by the **[school/setting]** unless permission has been given. This includes images shared through websites, social media, newsletters, learning journals, parent/carer platforms or other **[school/setting]** systems.

72. Parents/carers who attend activities, trips or events in an official or volunteer capacity are expected to follow the **[school/setting]** safeguarding, confidentiality, image use, acceptable use and data protection procedures. This does not prevent parents/carers from taking photographs or videos of their own child(ren) for personal and family use where this is permitted by the **[school/setting]**. Parents/carers and volunteers should not take photographs or recordings on behalf of the **[school/setting]**, or of other child(ren) in their volunteer capacity, using personal devices. ***Note: Amend as appropriate, for example if leaders decide to permit this in exceptional circumstances. Where permitted, this should be explicitly agreed in advance, risk assessed, documented and managed in line with school/setting procedures. Arrangements should include the purpose of the images, consent/lawful basis, authorised device, transfer, storage, deletion and confirmation that images must not be retained, copied, uploaded, posted or shared by the parent/carer or volunteer for any personal purpose***

73. Any concerns about photography, filming or the sharing of images should be reported to the DSL, DPO, headteacher/manager or another relevant senior leader.

Use of images by children

74. **[School/setting name]** will discuss and agree age-appropriate acceptable use rules with child(ren) regarding the use of cameras and devices, including where and when images may be taken. This will include places children cannot take cameras, for example unsupervised areas, toilets etc.

75. Child(ren) will be taught, in an age-appropriate way, to ask permission before taking images of others and to understand that everyone has the right to say no to being photographed or recorded.

76. Child(ren) will not be permitted to use cameras or image-capturing devices in sensitive areas such as toilets, changing areas, sleeping areas, swimming areas or other spaces where privacy and dignity may be compromised.

77. The use of personal devices by child(ren), including mobile phones, wearable technology, tablets, digital cameras and smart technology, is covered within the **[school/setting]** mobile phone and smart technology policy and acceptable use arrangements. ***Amend as appropriate***

78. Staff will ensure child(ren) are appropriately supervised when taking images for official or curriculum use.

79. Images taken by child(ren) for official **[school/setting]** use will be treated as setting-controlled image use and will be managed in line with this policy.

80. Parents/carers will be informed where child(ren) may take images of other child(ren) as part of setting-led learning activities, and how these images will be managed.

81. Images taken by child(ren) for official or curriculum use will be checked before being displayed, shared with parents/carers, uploaded to online systems or shown on digital screens.

Use of images of children by the media/press

82. Where press or media attendance is planned, **[School/setting name]** will consider carefully how access will be managed before any photography, filming or interviews take place.

83. Images taken by the press or media may be published more widely than **[school/setting]**-controlled images, including online, in print and through social media channels. Once published, the **[school/setting]** may have limited control over how images are shared, copied or reused.

84. Appropriate consent will be obtained before child(ren) are photographed, filmed or interviewed by the press or media. Where a parent/carer does not give consent, or where a child does not wish to be involved, this will be respected.

85. Particular care will be taken where child(ren), families or staff may be more vulnerable if identified, including child(ren) in care, adopted child(ren), child(ren) subject to safeguarding plans or court orders, or families affected by domestic abuse, stalking, harassment or other safety concerns.

86. Press and media organisations may process personal information for journalistic purposes, and data protection law includes exemptions in some circumstances for journalism. However, this does not remove the **[school/setting]** responsibility to manage access to child(ren) safely, check consent, consider safeguarding risks and communicate clearly with families.

87. Where press or media attendance is planned, **[School/setting name]** will agree expectations in advance. This may include confirming who will attend, checking identification on arrival, agreeing which child(ren) may be photographed or interviewed, limiting detailed captions,

avoiding full names where possible, and ensuring staff are available to supervise media activity.

88. The identity of any press representative will be verified on arrival. Access will only be permitted where the event is planned and where press or media representatives have been specifically invited to attend.

89. Unscheduled press or media visits will not be authorised without approval from the **[headteacher/manager]** or other designated senior leader.

Use of external photographers, **including videographers and volunteers**

90. External photographers engaged to record events or take images on behalf of [**School/setting name]** must agree to work in line with the **[school/setting]** safeguarding, image use, confidentiality and data protection expectations.

91. Where an external photographer processes images on behalf of the **[school/setting]**, the **[school/setting]** will usually remain responsible for deciding why and how images are used. In these circumstances, the photographer or videographer is likely to be acting as a data processor, and a written contract/agreement will be in place, so both parties understand their responsibilities and liabilities. The agreement will make clear the purpose of the photography /filming, what images may be taken, how they will be stored, who may access them, how long they will be retained and how they will be securely deleted or returned to the **[school/setting]**.

92. Images taken by external photographers must not be used for any other purpose, shared with third parties, uploaded to personal or unauthorised platforms, or used in the photographer's own publicity unless this has been specifically agreed and appropriate consent is in place.

93. **[School/setting name]** will satisfy itself that any external photographer can handle images safely and securely, including in relation to confidentiality, secure storage, transfer of images, deletion arrangements, use of assistants/sub-contractors and any online galleries or ordering systems.

94. External photographers will not have unsupervised access to child(ren).

95. Staff, parents/carers or volunteers taking photographs or videos on behalf of the **[school/setting]** will be treated as acting in an official capacity and must follow the [**school/setting]** safeguarding, confidentiality, image use and data protection expectations. In these cases, official images will be taken, stored and transferred using **[school/setting]**-approved equipment, accounts and systems.

Policy breaches and concerns

96. Members of the **[school/setting]** community should report concerns about image use or breaches of this policy in line with existing procedures. This may include reporting to the **[headteacher/manager]**, DSL, DPO or another designated senior leader, and following child protection, data protection, behaviour, complaints, whistleblowing or other relevant procedures. ***Amend as appropriate***

97. If **[School/setting name]** becomes aware that an image or video of a child or member of staff has been misused, altered, shared without consent, used in a threat, or used in a way that raises concern, this will be treated as a safeguarding and/or data protection concern and/or criminal offence as appropriate.

98. The **[school/setting]** will prioritise the safety, dignity and emotional wellbeing of any child or adult affected.

99. Staff will report any concerns immediately to the DSL, DPO and/or senior leadership team, in line with child protection, data protection, behaviour, whistleblowing and complaints procedures as appropriate.

100. The **[school/setting]** will record the concern and consider whether a safeguarding issue, criminal offence and/or personal data breach has occurred.

101. The **[school/setting]** will seek appropriate advice and make referrals or reports to relevant agencies where required. This may include children's social care, the police, the Local Authority Designated Officer (LADO), the ICO or other commissioned legal/data protection advisers.

102. Staff should not copy, forward, screenshot, download, save, print, further share or delete relevant content unless advised to do so by an appropriate safeguarding, police or data protection professional. Where evidence needs to be preserved, this should be done securely, proportionately and only by authorised staff.

103. Where threats, blackmail, extortion or suspected criminal activity are involved, the [**school/setting]** will seek urgent police and safeguarding advice and will not engage with demands made by individuals attempting to exploit or threaten the **[school/setting]** community.

104. The **[school/setting]** will consider immediate steps to reduce further access to relevant images. This may include removing images from **[school/setting]**-controlled platforms, requesting removal from websites or social media services, restricting access, reviewing whether a data breach assessment is required, and identifying what support is needed for affected child(ren), families and staff.

105. Following any breach or concern, leadership staff will review what happened, support affected individuals and consider whether changes are needed to policy, consent processes,

staff training, image storage, website/social media use, platform controls or wider safeguarding practice.

106. 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, behaviour, staff conduct, allegations, low-level concerns, whistleblowing, complaints and disciplinary policies. ***Amend as appropriate***

Template FAQs for Parents and Carers

Why does our school/setting need an image use policy?

Photographs and videos are often used in education settings to celebrate children's achievements, record learning, share special events and promote the life of the school/setting. Families often value seeing these moments in displays, newsletters, websites or other communications.

Our image use policy helps us make sure photographs and videos are taken, stored and shared safely, respectfully and lawfully. It also helps parents/carers make informed decisions about consent.

What are the risks?

Most images are used positively and safely. However, sharing images publicly can sometimes create risks, particularly where a child, family member or member of staff can be identified.

For example, some children, families or staff may be at risk if their image or location is shared publicly. This may include children in care, adopted children, families who have fled domestic abuse, or adults and children experiencing harassment, stalking or unwanted contact. In some cases, images may also attract the attention of people who may seek to harm or exploit children.

There are also newer online risks. Images shared online may be copied, saved, altered or misused without permission. National guidance has highlighted concerns about publicly available images being manipulated using artificial intelligence and other digital tools.

These risks are not intended to cause unnecessary alarm, but they are important to consider so that images can be used in a safe and proportionate way.

Why are education settings reviewing how images are shared?

The online environment has changed. Once an image is shared publicly, it can be difficult to control how it is copied, downloaded, shared or reused. This does not mean we should stop using images altogether, but it does mean we need to think carefully about when, where and how they are shared.

We will consider whether public sharing is necessary, whether a less identifiable image could be used, and whether safer options are available, such as secure platforms, images of activities or work, or group images where children are less identifiable.

What about the school/setting website and social media?

Where we use images on our official website, social media or other public channels, we will take steps to reduce risk. This may include avoiding children's full names, limiting identifying information, using images where children are less identifiable, checking consent, removing metadata where possible and regularly reviewing images so they are not kept online longer than necessary.

If a child is pictured, we will usually avoid naming them. If a child is named, we will usually avoid using their image.

Can I take photos or videos of my child at school/setting events?

Parents/carers often want to take photos or videos of their own children at events such as performances, sports days or celebrations. The Information Commissioner's Office explains that data protection law does not stop parents/carers taking photos or videos for their own personal or household use. However, schools and settings can set their own expectations for safeguarding, child protection, privacy or health and safety reasons.

The concern is usually not parents taking photos of their own child for personal memories. The concern is when photos or videos also include other children, staff or families and are then shared more widely, especially on social media. You may not know who is vulnerable, who does not want their image shared, or where sharing an image could create a safeguarding or privacy concern.

Sharing images privately with close family and friends is usually likely to remain personal use. However, sharing images publicly, or with an indefinite number of people, may go beyond personal use. The safest approach is not to share photos or videos publicly if they include other people's children, unless you have their parent/carer's permission.

What can parents/carers do to help?

You can help us keep children, families and staff safe by respecting our image use policy, following any instructions at events, not sharing images of other people's children publicly, and speaking to us if you have any concerns about your child's image being used.

If your family circumstances change, or if you wish to change or withdraw consent, please let us know in writing so that we can update our records.

Parental Consent for Images - Template Letter

Dear Parent/carer

At **[School/setting name]** we sometimes use photographs and videos to record learning, celebrate achievements, share special events and reflect the wider life of our **[school/setting]**. Images can be a positive way of helping children and families remember experiences, recognise progress and feel part of the **[school/setting]** community.

Images may be used in displays, newsletters or printed publications, learning journals, secure parent/carer platforms, our official website or social media channels, and for media or publicity where appropriate. ***Amend as appropriate to reflect setting decisions***

Images of identifiable children are personal data and must be handled carefully in line with data protection legislation, including the UK GDPR and the Data Protection Act 2018. We are asking you to complete the attached consent form so that we know how you are happy for your child's image to be used.

Some images may also be used for necessary internal educational, safeguarding, security or administrative purposes. Where this applies, the school/setting will identify an appropriate lawful basis and ensure images are handled securely, accessed only by those who need to see them, and used only where necessary and proportionate.

We recognise that images shared online may be copied, saved, altered or misused without our knowledge, including through artificial intelligence or other digital tools. We therefore take a safeguarding-led approach to image use and will consider whether an image is necessary, how identifiable children are, where it will be shared, how long it will be kept and whether a safer alternative could be used. Where possible, we will avoid using children's full names alongside their images.

We understand that some families may have particular reasons for wanting to protect a child's identity, including safeguarding, family, cultural, religious, privacy or personal reasons. If circumstances change, or if you wish to refuse, restrict or withdraw consent at any time, please let us know in writing so that we can update our records.

Where appropriate, we encourage you to talk to your child about the consent choices, as children should be involved in decisions about how their images are used wherever possible.

Our relevant policies, including image use, online safety and mobile/smart technology, are available on request or via **[insert location/link]**.

Please read and complete the attached form. If you have any questions or would like to discuss your child's image use, please contact us.

Yours sincerely,

[Name]
[Headteacher/Manager]

Parental Consent for Images - Template Form

Parental Consent for Use of Images at [school/setting name]

Please complete this form to let us know how you are happy for your child's image to be used.
Note: Settings should amend the following content and statements to reflect their individual leadership and policy decisions. Settings should ensure that consent choices are recorded clearly, are accessible to relevant staff, checked before images are used, and updated promptly if consent is changed or withdrawn. Any sensitive image-use concerns should be recorded separately and securely, with access limited to staff who need to know in order to safeguard the child or manage image use appropriately.

Conditions of use

- This consent will apply while your child attends **[School/setting name]**, unless you withdraw or change it sooner.
- Consent can be refused, restricted or withdrawn at any time by informing **[School/setting name]** in writing.
- Images of identifiable children are personal data. We will use the information on this form to record your consent choices and to help ensure images are taken, used, stored, shared and deleted in line with our safeguarding, image use and data protection procedures.
- Some images may be used for necessary internal educational, safeguarding, security or administrative purposes. These images will be handled in line with data protection legislation and the **[school/setting]** policies. They will be accessed only by those who need to see them, stored securely and used only where necessary and proportionate.
- We will not normally continue to use images of your child after they leave the **[school/setting]** unless we have a clear reason to do so and appropriate consent remains in place.
- Where children's images are published online, we will avoid using full names or unnecessary identifying information. In most cases, children who are pictured will not be named. If there is a clear reason to use a child's full name alongside their image, specific consent will be sought first.
- Where possible, we will use images that reduce identifiability, such as over-the-shoulder images, group photographs from a distance, images of activities, displays or children's work.
- We will only use images where children are appropriately dressed and where the image is suitable for the intended purpose.
- We will talk to children about image use in an age-appropriate way and take their wishes and feelings into account wherever possible.
- Images shared online may be copied, saved, altered or misused without the **[school/setting]** knowledge. We will take steps to reduce these risks, including limiting identifying information, considering safer image choices and reviewing images that are no longer needed.

- Images will be taken, stored, used, shared and deleted in line with our safeguarding, online safety, image use, data protection and other relevant policies***. Amend as appropriate to reflect setting policy titles.***
- Parents/carers are encouraged to contact us if they have any questions or concerns about image use, or if family circumstances change in a way that may affect consent.

Consent choices

Please circle your answer.
Note: Settings should amend as appropriate to reflect their policy decisions and systems

May we use your child's image in displays around the **[school/setting]**?	Yes / No
May we use your child's image in newsletters, printed publications, prospectuses or other materials produced by the **[school/setting]**?	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 specific social media channels]**	Yes / No
May we use, record or share your child's image as part of appropriately risk assessed and managed online learning, video conferencing or webcam-based curriculum activities? ***Amend as appropriate.***	Yes / No
May we use, record or share your child's image as part of online broadcasts or recordings of performances, assemblies, celebrations or events? ***Note: Settings should specify whether this includes livestreaming, pre-recorded content, the platform used, who can access it and how long recordings will be available.***	Yes / No
May your child appear in media coverage, for example where a newspaper photographer, journalist or television crew attends an event?	Yes / No
May we share your child's image with approved external providers for the following agreed **[school/setting]** purposes: **[insert purposes/providers]**. We will only do this where appropriate arrangements are in place to protect images and ensure they are used only for the agreed purpose. ***Amend as appropriate or remove if not applicable.***	Yes / No
May we share your child's image with parents/carers through our approved secure learning journal/parent/carer platform? **[Insert platform name]** ***Amend/remove as appropriate***	Yes / No

Parent/carer declaration

I/we have read and understood the information above and the accompanying letter.

I/we understand that public websites and social media can be viewed widely and that images shared online may be copied, downloaded, altered or reused without the **[school/setting]**'s knowledge or consent. I/we understand that the **[school/setting]** will take steps to reduce these risks, including limiting identifying information, reviewing where images are shared, using safer image choices where possible, and removing images when they are no longer needed or consent no longer applies.

I/we understand that where the press or media are invited to attend an event, the **[school/setting]** will seek appropriate consent and take reasonable steps to agree how children's names, images and other personal information will be used. I/we also understand that media organisations may process information for journalistic purposes.

I/we will discuss image use with my/our child where appropriate and support them to share their views.

I/we understand that if I/we take photographs or videos at **[school/setting]** events these should be for personal and family use only. If these photographs or videos include other children, staff or families, I/we understand these should not be shared publicly or uploaded to open social media without permission.

Restrictions, concerns or specific circumstances

If there are any restrictions, concerns or specific circumstances which may affect how your child's image is used, please contact us directly so that this can be discussed and recorded appropriately. Please do not include sensitive information on this form. ***Note: Settings should ensure that any sensitive image-use concerns are recorded securely and only shared with staff who need to know in order to safeguard the child or manage image use appropriately.***

Name of child: _____ Date: _____

Parent/carer name: _____

Parent/carer's signature: _____

Child's signature (if appropriate): _____

Group Activity - Template Letter and Forms

Dear Parent/Carer

We are holding **[production/special event name]** on **[date]**. We know that many parents and carers may wish to take photographs or videos of their own child during the event, and we understand that these can be special memories for families.

At **[School/setting name]** we have a policy in place regarding the taking, use and sharing of images. You will previously have been asked to complete a consent form setting out how your child's image may be used by the **[school/setting].**

Parents and carers may take photographs or videos of their own child at this event for personal and family use, unless we tell you otherwise. The concern is usually not parents taking images of their own child for personal memories, but where photographs or videos also include other children, staff, families or visitors and are then shared more widely, particularly online.

Some children, families or staff may be at risk if their image is shared publicly. This may include children in care, adopted children, families who have experienced domestic abuse, or adults and children who may be at risk of harassment, stalking or unwanted contact. Not all members of the community will know who may be vulnerable or who does not want their image shared.

Images and videos shared online may also be copied, saved, altered or misused without permission, including through artificial intelligence or other digital tools. Once an image has been shared publicly, it can be difficult to control how it is used.

For this reason, we ask that any photographs or videos taken at this event are for personal use only. Please do not share images or recordings publicly, or upload them to open social media, if they include other children, staff or families, unless you have permission from those involved or their parent/carer. Please also be aware that photographs or videos must not be taken for commercial purposes or with a view to selling or distributing recordings of the event.

If there are specific reasons why your child should not be photographed or filmed during the event, please let us know as soon as possible. Where concerns are raised, we will consider reasonable steps to support your child's involvement. This may include, where appropriate, seating arrangements, designated photography opportunities, reminders to the audience, or other practical arrangements. We will only restrict photography more generally where this is necessary to protect children, families, staff or the wider setting community.

We hope you will support us in helping everyone enjoy the event while respecting the privacy and safety of others.

Please complete and return the slip below by **[date]**. If you have any questions or concerns, please contact us.

Yours sincerely,

[Name], [Headteacher/Manager]

Parental response slip

Child's name: _____

Event: _____

Date: _____

Please tick:

☐ I understand the expectations regarding photographs and videos at this event.

☐ I would like to discuss a concern about my child being photographed or filmed.

Please do not include sensitive information on this slip. If you have a concern, we will contact you to discuss this through an appropriate route.

Parent/carer name: _____

Parent/carer signature: _____

Date: _____

Live Broadcasting - Template Letter and Forms

Dear Parent/Carer

We are holding **[production/special event name]** on **[date]**. This year, we plan to share the event online so that families who are unable to attend in person can still watch or listen to the event.

The event will be shared as follows: **[Insert details, for example whether the event will be livestreamed, pre-recorded and shared afterwards, the platform that will be used, who will be able to access it, any password/login arrangements, and the date/time of the broadcast.]**

If a recording will be available after the event, it will be available for: **[Insert details about how long the recording will be available and who will be able to access it. Remove this sentence if the event will be livestreamed only. Include whether parents/carers may download or save the recording, or whether viewing only is permitted.]**

At **[School/setting name]**, we have a policy in place regarding the taking, use and sharing of images. You will previously have been asked to complete a consent form setting out how your child's image may be used by the school/setting.

We know that sharing events online can be a positive way to include families and celebrate children's achievements. However, where events are livestreamed or recorded, images, video or audio may include other children, staff, families or visitors. Some children, families or staff may be at risk if their image or location is shared more widely. Not all members of the community will know who may be vulnerable or who does not want their image shared.

Images and recordings shared online may also be copied, saved, screenshotted, recorded privately, forwarded, altered or misused without permission, including through artificial intelligence or other digital tools. Once content has been shared beyond the intended audience, it can be difficult to control how it is used.

For this reason, we ask that any link, recording or access information shared with you is used only by the intended audience and is not passed on more widely. Images, recordings or screenshots from the event should not be shared publicly or uploaded to open social media if they include other children, staff or families.

You can support us by:

- keeping any link, password or access information private.
- not recording, copying, screenshotting or sharing the broadcast unless the **[school/setting]** has said this is permitted.
- not posting images or recordings from the event on public social media if they include other children, staff or families.
- letting us know if you have any concerns about your child being included in the broadcast or recording.

If content is shared or accessed outside these expectations, we may need to restrict or withdraw access to online events in the future. We hope you will support us in helping families enjoy the event while protecting the privacy and safety of children, staff and the wider setting community.

Please complete and return the slip below by **[date]**. If you have any questions or concerns, please contact us.

Yours sincerely,

[Name], [Headteacher/Manager]

Parental consent for children's images being shared online as part of an event

- I understand that **[School/setting name]** will be sharing **[event name]** online.
- The event will be: **[Insert details, for example livestreamed / pre-recorded / shared afterwards / audio only / available through a secure platform]**.
- The event will be available via: **[Insert platform, access arrangements, password/login requirements and intended audience].**
- The recording will be available for: **[Insert timeframe or remove if livestream only]. Include whether parents/carers may download or save the recording, or whether viewing only is permitted.**

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

- do not share links, passwords or access information with anyone outside the intended audience.
- do not make private recordings or screenshots unless the school/setting has said this is permitted.
- do not share images, recordings or screenshots publicly or upload them to open social media if they include other children, staff or families.

Please tick one:

☐ I am happy for my child to be included in the online sharing/broadcast/recording of this event.

☐ I am not happy for my child to be included in the online sharing/broadcast/recording of this event.

☐ I would like to discuss this with the school/setting before making a decision. **Please do not include sensitive information on this form. If you would like to discuss a concern, we will contact you directly.**

Child's name: _____Event/Date: _____

Parent/carer name: _____

Parent/carer signature: _____

Child's signature, if appropriate: _____

Template Posters for Education Settings

[Setting Logo]

[School/setting name] Guide to Using Images Safely and Responsibly

Photographs and videos are a lovely way to capture special moments, celebrate achievements and remember events. Families often value being able to take images of their own children at performances, sports days, celebrations and other school/setting events.

We are happy for parents/carers to take photographs and videos of their own child(ren) for personal and family use, unless we tell you otherwise. The concern is usually not families taking images for personal memories, but where photos or videos also include other children, staff, families or visitors and are then shared more widely, particularly online.

Please remember that not everyone wants, or is able, to have their image shared publicly. Some children, families or staff may be at risk if their image or location is shared. This may include children in care, adopted children, families who have experienced domestic abuse, or adults and children who may be at risk of harassment, stalking or unwanted contact. Not all members of the community will know who may be vulnerable or who does not want their image shared.

Images and videos shared online may also be copied, saved, altered or misused without permission, including through artificial intelligence or other digital tools. Once an image has been shared publicly, it can be difficult to control how it is used.

To help keep our whole community safe, please:

- take photographs and videos for personal and family use only;
- avoid sharing images publicly if they include other people's children, staff or families;
- do not upload images or videos to open social media if they include staff or other people's children without permission;
- follow any instructions given by staff at events;
- speak to us if you have any concerns about images being taken or shared.

Thank you for helping us celebrate special moments while respecting the privacy and safety of children, families and staff.

Further Information on the use of Images and video and online safety:

- Information Commissioner's Office: https://ico.org.uk/for-the-public/schools/photos
- NCA-CEOP: www.ceopeducation.co.uk/parents
- Internet Matters: www.internetmatters.org
- Childnet: www.childnet.com

[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 videos of their own child(ren) at this event for personal and family use.

Please remember that photos and videos may also include other children, staff, families or visitors. We ask that images are not shared publicly or uploaded to open social media if they include other people's children, staff or families without permission.

Some members of our community may be at risk if their image or location is shared.

Thank you for helping us respect and protect everyone.

[Headteacher/Manager]

Template Consent for Staff Images

[School/setting name] Staff Photograph and Image Consent Form

[School/setting name] may wish to use staff images for agreed [school/setting] purposes, such as staff recognition, internal displays, intranet/learning platforms, the [school/setting] website, newsletters or official social media channels.

Images of identifiable staff are personal data and must be handled in line with data protection legislation, including the UK GDPR and the Data Protection Act 2018. Consent should be specific, informed and capable of being withdrawn.

Please complete this form to let us know how you are happy for your image to be used.

Conditions of use

- This consent will apply for [insert timeframe, for example two years / the duration of employment / the duration of a specific project], unless you withdraw or change it sooner.
- Consent can be refused, restricted or withdrawn at any time by informing [insert contact/person/team] in writing.
- Some images may be used for necessary internal operational, security, safeguarding or administrative purposes, such as ID badges, access control, staff management systems, internal safeguarding or security records, or similar necessary internal uses. These uses may not rely on consent, but the [school/setting] will identify an appropriate lawful basis, handle images securely and use them only where necessary and proportionate.
- This consent form relates to optional uses of staff images, such as staff recognition, internal displays, website profiles, newsletters, publicity or social media.
- You do not have to agree to optional use of your image, and choosing not to give consent will not disadvantage you.
- Your image will only be used for the optional purposes you have agreed to on this form.
- We will not use your image for any other optional purpose without further consent, unless there is another clear and appropriate lawful basis for doing so.
- Where your image is published online, for example on the [school/setting] website or official social media channels, it may be viewed widely and could be copied, saved, altered or misused without the [school/setting]'s knowledge or consent. We will take reasonable steps to reduce risks, including limiting unnecessary identifying information, using appropriate images, reviewing images regularly and removing images when they are no longer needed or consent no longer applies.
- We recognise that some staff may have personal, safeguarding, privacy or safety reasons for not wanting their image used or published.
- Publication of your image will normally cease when you leave the [school/setting], unless there is a clear reason to retain or continue using it and appropriate consent or another lawful basis remains in place.

- Images will be taken, stored, used, shared and deleted in line with our data protection, safeguarding, online safety, image use, acceptable use, social media and mobile/smart technology policies. ***Amend as appropriate to reflect setting policy titles***.

Consent choices

Please circle your answer. ***Note: Settings should amend as appropriate to reflect their policy decisions and systems***

	Consent choice
May we use your image for optional internal staff recognition purposes, such as an internal staff board, intranet profile, learning platform or staff directory?	Yes / No
May we use your image in newsletters, printed publications, prospectuses or other **[school/setting]** materials?	Yes / No
May we use your image on our official website?	Yes / No
May we use your image on our official social media channels? **[List channels]**	Yes / No
May we use your image in press/media coverage of **[school/setting]** events?	Yes / No
May we share your image with approved external providers for agreed **[school/setting]** purposes, where appropriate safeguards are in place? ***Amend/remove if not applicable.***	Yes / No

Staff declaration

- I have read and understood the information above.
- I understand that images published online may be viewed widely and could be copied, saved, altered or reused without the **[school/setting]**'s knowledge or control. I understand that the **[school/setting]** will take reasonable steps to reduce these risks, such as limiting identifying information, using safer image choices where possible, and reviewing or removing images when they are no longer needed.
- I understand that I can refuse, restrict or withdraw consent at any time by informing **[insert contact/person/team]** in writing.
- I understand that if I withdraw consent, the **[school/setting]** will stop using my image for future purposes and will take reasonable steps to remove it from **[school/setting]**-controlled platforms where practicable. I understand that it may not always be possible to remove images that have already been printed, distributed, archived or shared by third parties.

If there are any restrictions, concerns or specific circumstances which may affect how your image is used, please contact **[insert contact/person/team]** directly so this can be discussed sensitively and recorded appropriately. **Please do not include sensitive information on this form.**

Name: _____

Signed: _____Date: _____

Acknowledgements

This guidance has been developed by the Kent County Council LADO Education Safeguarding Advisory Service, drawing on previous guidance produced with input from the Kent County Council Information Governance Team.

Earlier versions of this document have drawn on, adapted or been informed by guidance and resources produced by a range of organisations. We gratefully acknowledge the contribution of materials and guidance from:

- Hampshire County Council
- Herefordshire Grid for Learning / Schools e-Safety Team
- Information Commissioner's Office
- UK Safer Internet Centre
- South West Grid for Learning
- Plymouth City Council

References to external organisations are included to acknowledge source material and wider sector guidance. Education settings should always ensure that any guidance they rely on is current and appropriate to their own context.