

Balcombe C E (C) School



Photographic and Images Policy

Adopted by Governors:

March 23

Reviewed:

March 24, May 25, May 26

Next Review:

May 27

Contents:

Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Definitions](#)
4. [Consent](#)
5. [General procedures](#)
6. [Additional safeguarding procedures](#)
7. [Online Safety and Image Sharing](#)
8. [Use of digital cameras](#)
9. [Other school-owned devices](#)
10. [Storage and retention](#)
11. [Appropriate use of images under UK GDPR and the DPA 2018](#)
12. [Use of cameras and filming equipment by parents](#)
13. [Use of cameras and filming equipment by pupils](#)
14. [Use of a professional photographer](#)

Statement of intent

At Balcombe C E Primary School we use images and videos for a variety of purposes, including prospectuses, display boards, educational purposes, School twitter, Facebook page and our website. We understand that parents may also wish to take videos or photos of their children participating in school events for personal use.

Whilst we recognise the benefits of photography and videos to our school community, we also understand that these can have significant risks for those involved. Under the legal obligations of the UK GDPR and the Data Protection Act (DPA) 2018, the school has specific responsibilities in terms of how photos and videos are taken, stored and retained.

The school has implemented a policy on the safe use of cameras and recording equipment by staff, pupils and parents to reflect the protective ethos of the school with regard to pupils' safety.

In order to ensure that, as far as possible, the use of photography and video is safe at all times, the policy provided below should be followed. This policy is applicable to all forms of visual media, including film, print, video, DVD and websites.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- The Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- DfE (2025) 'Keeping children safe in education 2025'
- The Equality Act 2010
- The Education (Pupil Information) (England) Regulations 2005
- The Online Safety Act

This policy operates in conjunction with the following school policies and consent forms:

- Data Protection Policy
- Anti-bullying policy
- Online safety Agreement
- Photography and video parental consent form

2. Roles and responsibilities

The headteacher and/or Business Manager are responsible for:

- Submitting consent forms to parents, and pupils where appropriate, at the beginning of Primary School life with regard to photos and videos being taken whilst at school.
- Ensuring that all photos and videos are stored and disposed of correctly, in line with the UK GDPR and the DPA 2018.
- Deciding whether parents are permitted to take photos and videos during school events.
- Communicating this policy to all the relevant staff members and the wider school community, such as parents.

The DSL is responsible for:

- Liaising with social workers to gain consent for the use of photos and videos of pupils who are LAC (Looked after child).
- Liaising with the DPO (Data protection Officer) to ensure there are no data protection breaches.
- Informing the headteacher of any known changes to a pupil's security, e.g. child protection concerns, which would mean that participating in photography and video recordings would put them at significant risk.

Parents and pupils are responsible for:

- Completing a google photography consent form.
- Informing the school in writing if they wish to make any changes to their consent.

- Acting in accordance with this policy.

3. Definitions

“Camera” is used to refer to mobile phones, tablets, webcams, portable gaming devices, and any other equipment or devices which may be used to take photos.

“Personal use” of photography and videos is defined as the use of cameras to take images and recordings of children by relatives, friends or known individuals, e.g. a parent taking a group photo of their child and their friends at a school event. These photos and videos are only for personal use by the individual taking the photo and are not intended to be passed on to unknown sources. The principles of the UK GDPR and the DPA 2018 do not apply to images and videos taken for personal use.

“Official school use” is defined as photography and videos which are used for school purposes. These images are likely to be stored electronically alongside other personal data. The principles of the UK GDPR and the DPA 2018 apply to images and videos taken for official school use.

“Media use” is defined as photography and videos which are intended for a wide audience, e.g. photos of children taken for a local newspaper. The principles of the UK GDPR and the DPA 2018 apply to images and videos taken for media use.

Staff may also take photos and videos of pupils for **“educational purposes”**. These are not intended for official school use, but may be used for a variety of reasons, such as school displays, special events, assessment and workbooks. The principles of the UK GDPR and the DPA 2018 apply to images and videos taken for educational purposes.

4. Consent

All photos and video content are classified as personal data under the UK GDPR and the DPA 2018; images or video content may be used for publicity or other purposes only once informed consent has been provided, and it has not been withdrawn.

Staff, pupils and parents will be encouraged to read the Data Protection Policy for more information on the school’s approach to data protection.

Parents and pupils will be aware that their child may be photographed at school and they have the right to withdraw consent for:

- Photos or videos taken by members of staff for school-based publicity and promotional purposes or for anonymous use on the school website.
- Photos or videos taken by parents and other family members of children at the school during school concerts, performances, sports events and other similar events organised by the school.
- Photos or video taken by members of the press who are on the school premises by invitation in order to celebrate individual, group or school success.

The school will recognise that consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Where consent is given, a record will be kept documenting how and when consent was given and last updated. The school will never assume consent if no response is received. We will make every effort to ensure we get a response from parents/carers, including following up with emails or calls.

The school will ensure that consent mechanisms meet the standards of the UK GDPR and the DPA 2018. Where the standard of consent cannot be met, an alternative legal basis for processing the data will be found, or the processing will cease.

Parents will be asked on behalf of Pupils to complete the photography consent form when their child starts school, which will determine whether or not they allow their child/themselves to participate in photos and videos.

The photography consent form will be valid for the time the child is at Balcombe CE Primary School, unless the pupil's circumstances change in any way, e.g. if their parents separate, or consent is withdrawn. Additional consent forms will be required if the pupil's circumstances change.

If there is a disagreement over consent, or if a parent/pupil does not respond to a consent request, it will be treated as if consent has not been given and photos and videos will not be taken or published of the pupil without consent.

All parents and pupils will be entitled to withdraw or change their consent at any time during the school year. Parents or pupils who wish to withdraw their consent must notify the school in writing.

If any parent or pupil withdraws or changes their consent, or the DSL reports any changes to a pupil's security risk, or there are any other changes to consent, the list will also be updated and re-circulated.

For any pupils who are LAC, PLAC, or adopted, the DSL will liaise with the pupil's social worker, carers or adoptive parents to establish where consent should be sought. Consideration will be given as to whether identification of pupils who are LAC, PLAC, or adopted would risk their security in any way.

Consideration will also be given to any pupils for whom child protection concerns have been raised. Should the DSL believe that taking photos and videos of any pupils would put their security at further risk, greater care will be taken towards protecting their identity.

A list of all the names of pupils for whom consent was not given will be created by the Office and will be accessible to all staff members. This list will be updated as required.

5. General procedures

Photos and videos of pupils will be carefully planned before any activity and the staff member in charge will oversee the planning of any events where photos and videos will be taken.

Where photos and videos will involve pupils who are LAC, PLAC, or adopted, or pupils for whom there are security concerns, the headteacher will liaise with the DSL to determine the steps involved.

The list of all pupils who have not consented to being photographed or recorded will be checked prior to the activity. Only pupils for whom consent has been given will be able to participate.

The staff members involved, alongside the headteacher, will liaise with the DSL if any pupil who is LAC, PLAC, adopted, or for whom there are security concerns.

A school-owned digital camera/I Pad will be used to take photos and videos of pupils.

Staff will ensure that all pupils are suitably dressed before taking any photos or videos.

Where possible, staff will avoid identifying pupils by name or any other identifiable data. If names are required, only first names will be used.

The school will not use photos or videos of:

- Any pupil who is subject to a court order.
- Children who have left the school, without the consent of their parents or, where appropriate, the children themselves.
- Staff members who have left the school, without their consent.

Photos and videos that may cause any distress or embarrassment will not be used.

Any concern relating to inappropriate or intrusive photography or publication of content will be reported to the DPO.

6. Additional safeguarding procedures

The school will consider certain circumstances that may put a pupil's security at greater risk and, thus, may mean extra precautions are required to protect their identity.

The DSL will, in known cases of pupils who are LAC, PLAC or adopted, liaise with the pupil's social worker, carers or adoptive parents to assess the needs and risks associated with the pupil.

Any measures required will be determined between the DSL, social worker, and carer and/or adoptive parent with a view to minimising any impact on the pupil's day-to-day life. The measures implemented will be one of the following:

- Photos and videos can be taken as per usual school procedures
- Photos and videos can be taken within school for educational purposes and official school use, e.g. on registers, but cannot be published online or in external media
- No photos or videos can be taken at any time for any purposes

Any outcomes will be communicated to all staff members via e mail and the list outlining which pupils are not to be involved in any videos or photos, held in the school office, will be updated accordingly.

7. Online Safety and Image Sharing

Online safety is a running and interrelated theme in our safeguarding approach. The school has a clear policy on the use of mobile and smart technology, reflecting that many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school, may sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content.

The school recognises that images and photographs can be misused online in several ways that pose safeguarding risks to children:

Risks associated with image sharing

Consensual and non-consensual sharing of images: Sexual violence and sexual harassment can occur online and face-to-face (both physically and verbally) and are never acceptable. The school has a zero-tolerance approach to sexual violence and sexual harassment. It is never acceptable and will not be tolerated. It will never be passed off as "banter", "just having a laugh", "a part of growing up" or "boys being boys". Failure to do so can lead to a culture of unacceptable behaviour, an unsafe environment and in worst case scenarios a culture that normalises abuse. Keeping Children Safe in Education

This includes:

- Consensual and non-consensual sharing of nude and semi-nude images and/or videos (often via large chat groups)
- Images being shared more widely than originally intended
- Images being manipulated or taken out of context to harass or bully pupils

Images shared by parents on social media: Parents should be aware that images shared on social media platforms can:

- Be accessed by unknown individuals if privacy settings are not properly configured
- Be copied, downloaded and shared without permission
- Remain online permanently, even if the original post is deleted
- Put children at risk if they reveal identifying information such as school uniform, location or routines

AI-generated images and deepfakes: The school is aware of emerging risks including:

- The creation of manipulated or 'deepfake' images using artificial intelligence
- Creating or sharing 'deepfake' pornography of someone without permission, which is a criminal offence under the Online Safety Act 2023 The Key Leaders
- The potential for images to be used to create fake or misleading content

How the school manages these risks

On school premises: The school carefully considers how mobile and smart technology is managed on our premises and reflects this in our mobile and smart technology policy and our child protection policy. Keeping Children Safe in Education

Education and awareness:

- Pupils are taught about how to keep themselves and others safe, including online, through our relationships and sex education (RSE) and personal, social, health and economic (PSHE) education. The Key Leaders
- Pupils are taught about the risks of sharing images online, including:
 - The permanence of online content
 - How to use privacy settings appropriately
 - The importance of consent
 - How to report concerns about inappropriate images

Working with parents: The school will:

- Communicate regularly with parents about online safety, including the risks associated with sharing images on social media
- Provide guidance on appropriate privacy settings and safe sharing practices
- Reinforce the importance of considering whether images should be shared publicly
- Remind parents that images shared at school events should be for personal use only and not shared on social media or other public platforms

Reporting and responding to concerns:

- All staff are aware of systems within the school which support safeguarding, including the child protection policy and online safety procedures. All staff receive appropriate safeguarding and child protection training (including online safety) at induction and regular updates. Keeping Children Safe in Education
- Any concerns about inappropriate use of images, including cyber-bullying, sexual harassment, or the sharing of nude or semi-nude images, should be reported immediately to the DSL
- The school will follow the procedures set out in our child protection policy and will work with external agencies where appropriate, including police and children's social care

Staff responsibilities: All staff should:

- Be vigilant about how images are used and shared
- Understand the risks associated with online image sharing

- Report any concerns about inappropriate use of images immediately
- Model appropriate behaviour in their own use of technology and images

Staff use of images:

All images taken by members of staff or volunteers at school or during school activities remain the property of the school and images must not be shared with anyone outside the school or held for private use.

No digital image will be uploaded onto any internet/intranet system without the express permission of the child's parent. Unless specific prior consent has been obtained, members of staff and volunteers will not post school images on personal pages of social networking sites or other websites.

Images will not be emailed or shared via private email accounts unless a parent has asked for a photo of their child to be sent to them.

This approach is reflected in our child protection policy, online safety policy, and mobile and smart technology policy, which should be read in conjunction with this Photography and Images Policy.

8. Use of digital cameras

Staff members may be provided with a camera or I Pad to record and maintain pictorial evidence of the lessons, behaviour, activities and events related to their pupils. Photos and videos may only be taken for educational purposes and in "school or educational provision settings" as mentioned above.

The use of personal cameras, mobile phone cameras or other recording equipment will be prohibited on school premises at all times.

The school-owned I Pads will be located and stored securely in the school office or charging trolley. Members of staff will be responsible for making sure that the I Pad is locked away after use, at the end of the day. Members of staff will not be allowed to take school I Pads or memory cards home.

Members of staff will not be allowed to bring in personal cameras without prior permission. If personal cameras are allowed to be brought in due to a specialist requirement or defective equipment, the memory card should be shown to be empty and images downloaded to the school's server.

Staff or other adults will not be permitted to take photos of pupils in vulnerable circumstances, such as when they are upset or inappropriately dressed. Members of staff and the school community will be required to report inappropriate use of digital cameras and images to the headteacher. If it is found that any incidents raise child protection concerns, immediate action will be taken in consultation with the DSL.

The school will not take responsibility for lost, stolen or damaged camera or electronic equipment. This remains the responsibility and obligation of the individual who has borrowed the equipment.

9. Other school-owned devices

Where school-owned devices other than digital cameras are used, images and videos will be provided to the school at the earliest opportunity and then removed from the devices.

Photos and videos taken by staff members on school visits may be used for educational purposes, e.g. on displays or to illustrate the work of the school, where consent has been obtained.

10. Storage and retention

As per the UK GDPR and the DPA 2018, images obtained by the school will not be kept for longer than necessary; retention periods for the different types of personal data are outlined in the ICO retention guidelines for schools.

Hard copies of photos and video recordings held by the school will be annotated with the date on which they were taken and will be stored in the school office. They will not be used other than for their original purpose, unless permission is sought from the headteacher and parents of the pupils involved and the DPO has been consulted.

Digital photos and videos held on the school's drive are accessible to staff only. Photos and videos are stored in labelled files, annotated with the date, and are only identifiable by year group or class number – no names are associated with images and videos. Files are password protected and only staff members have access to these passwords.

Paper documents will be shredded or pulped and electronic memories scrubbed clean or destroyed once the retention period has ended. The DPO will review stored images and videos on an annual basis to ensure that all unwanted material have been deleted.

Where a parent or pupil has withdrawn their consent, any related imagery and videos involving their child/the pupil will be removed from the school drive immediately. When a parent withdraws consent, it will not affect the use of any images or videos for which consent had already been obtained. Withdrawal of consent will only affect further processing.

Where a pupil's security risk has changed, the DSL will inform the headteacher immediately. If required, any related imagery and videos involving the pupil will be removed from the school drive immediately. Hard copies will be removed by returning them to the parent/pupil or by shredding, as appropriate.

Official school photos will be held on Bromcom alongside other personal information and retained for the length of the pupil's attendance at the school, or longer if necessary, e.g. due to a police investigation.

Images taken on school cameras or I Pads will be downloaded as soon as possible on to a school server, ideally once a week.

Members of staff will maintain responsibility for ensuring that images are safely stored, particularly on memory sticks and hard drives. They will take reasonable measures to ensure that they do not come into the possession of unauthorised persons.

No digital image will be altered or enhanced in any way by any member of staff, unless given prior permission by the headteacher to do so. The school may require images to be deleted or edited as appropriate and may choose to use images taken by members of staff or volunteers for other purposes, provided the processing conditions and consent requirements of this policy are met. Staff members are responsible for ensuring that edited images do not mislead or misrepresent. They must not edit images which result in their subject being vulnerable to embarrassment, teasing, bullying or abuse.

If the memory card for individual school cameras needs to be replaced, then the replaced memory card will be destroyed to ensure that no images can be recovered. Members of staff must remember that, even when images are physically deleted from a camera or memory card, the camera or the memory card must be appropriately disposed of to ensure that no imprint remains.

11. Appropriate use of images under UK GDPR and the DPA 2018

Photos will be used in school for many reasons and the different uses for the same image should be considered separately, as each photograph and use will potentially have different conditions for processing.

As a public body, the school will consider whether the processing is taking place in the performance of its duties as a public authority. Where this is the case, the legal basis for processing will be recorded as 'public task', not 'legitimate interests' – public authorities cannot use legitimate interests as a lawful basis if the processing is in the performance of their tasks as a public authority.

The school will use privacy notices with declarations attached to inform staff, pupils and parents about how their personal data may be collected and as one method of gaining consent.

To judge whether legitimate interest can be used as the basis for processing data, the school will carry out three different tests. These are:

- A purpose test – establishing the reasons for using the data, what will be achieved and whether the benefits are justifiable.
- A necessity test – establishing whether the processing of pupils' data will be useful and whether there is a less intrusive way of reaching a means to an end.
- A balance test – establishing the impact it will have on the data subject by processing the data for said reason.

These three tests make up a 'legitimate interest assessment' (LIA) – the school will carry out an LIA prior to obtaining the data and it will be recorded in a physical copy in compliance with the UK GDPR and the DPA 2018.

Photos used in identity management

These are likely to be essential for performing the public task of the school, but they will be deleted once the child is no longer in attendance – as they are no longer needed for the purpose for which they were held.

Photos used for marketing purposes

Photos will not be used for marketing purposes unless the school has specific informed consent for the images and the images are only used in line with the consent provided.

The school will recognise that when images are posted on the school website or social media anyone may view the images, and consequently this may result in a greater risk of misuse of images. The school will therefore give specific consideration to the suitability of images for use on the school's website and social media.

Photos in the school environment relating to education

These photos may be essential for performing the public task of the school. If the school wishes to display the image with good reason beyond the pupil's time at the school, this must be deleted if requested by the parent.

12. Use of cameras and filming equipment by parents

Parents or family members will be welcome to take photos of (and where appropriate, film) their own children taking part in schools events, subject to the following guidelines, which the schools expects all parents to follow. Parents will:

- Remain seated while taking photos or videos during concerts, performances and other events.
- Minimise the use of flash photography during performances.
- In the case of all school events, make the focus of any photos and/or videos their own children.
- Avoid disturbing others in the audience or distracting pupils when taking photos or recording videos.
- Ensure that any images and recordings taken at school events are exclusively for personal use and are not uploaded to the internet, posted on social networking sites or openly shared in other ways.
- Refrain from taking further photos and/or videos if and when requested to do so by staff.
- Many children have unlimited access to the internet via mobile phone networks, and images shared online can be misused for sexual harassment, bullying, or control
- Images should not be shared publicly on social media where they can be accessed by unknown individuals
- Parents should consider privacy settings carefully before posting any images

13. Use of cameras and filming equipment by pupils

All pupils will be encouraged to look after each other, and to report any concerns about the misuse of technology, or any worrying issues to a member of staff.

The use of cameras, or filming equipment, including on mobile phones, will not be allowed in toilets or changing areas, nor should photography or filming equipment be used by pupils in a manner that may offend or cause upset.

Misuse of images, cameras, or filming equipment in a way that breaches this policy, or the school's Anti-bullying Policy and Internet Acceptable Use Agreement, will always be taken seriously and may be the subject of disciplinary procedures or dealt with under the relevant safeguarding policy as appropriate

14. Use of a professional photographer

If the school decides to use a professional photographer for official school photos and school events, the headteacher will:

- Provide a clear brief for the photographer about what is considered appropriate, in terms of both content and behaviour.
- Issue the photographer with an identification badge or card, which must be worn at all times.
- Let pupils and parents know that a photographer will be in attendance at an event and ensure they have previously provided consent to both the taking and publication of videos and/or photos.
- Not allow unsupervised access to pupils or one-to-one photo sessions at events.
- Communicate to the photographer that the material may only be used for the school's own purposes and that permission has not been given to use the photos for any other purpose.
- Ensure that the photographer will comply with the requirements set out in the UK GDPR and the DPA 2018.
- Ensure that if another individual, such as a parent or governor, is nominated to be the photographer, they are clear that the images and/or videos are not used for anything other than the purpose indicated by the school.

This policy will be reviewed annually by the Headteacher/School Business Manager, in consultation with the DSL and DPO, to ensure it remains compliant with current legislation and guidance.

Our DPO is Darren Carpenter and is contactable via DCarpenter@hurst.education