

Loxwood Primary School

Photograph, Filming and Social Media Policy



Approved by:

Governing Body

Date: September 2025

Next review due by:

September 2027

1. Aims

The purpose of this policy statement is to:

- protect children and young people who attend Loxwood Primary School, specifically those where photographs and videos may be taken
- set out the overarching principles that guide our approach to photographs/videos being taken of children and young people during our events and activities
- ensure that we operate in line with our values and within the law when creating, using and sharing images of children and young people.

This policy statement:

- Applies to all staff and to all online communications which directly or indirectly, represent the school.
- Applies to such online communications posted at any time and from anywhere.

2. Legislation and guidance

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. Summaries of key legislation and guidance is available on NSPCC Learning: Online abuse legislation and guidance. Child protection legislation and guidance.

3. Responsibilities

We believe that:

- children and young people should never experience abuse of any kind
- we have a responsibility to promote the welfare of all children and young people and to take, share and use images of children safely.

We recognise that:

- sharing photographs and films of our activities can help us celebrate the successes and achievements of our children and young people, provide a record of our activities and raise awareness of our organisation
- the welfare of the children and young people taking part in our activities is paramount
- children, their parents and carers have a right to decide whether their images are taken and how these may be used, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation
- consent to take images of children is only meaningful when children, their parents and carers understand how the images will be used and stored, and are fully aware of the potential risks associated with the use and distribution of these images
- there are potential risks associated with sharing images of children online.

“Any image or video content shared on a social media platform set to public can be accessed by anyone. Schools should exercise great caution sharing images or videos of learners publicly on social media platforms due to the potential risk of the content being misused. Social media platforms can be vulnerable to web scraping which facilitates public content to be collected at scale. Loss of control of images, for example, can expose learners to potential data and privacy risks”. [HwB: Practices and principles for schools’ use of social media](#)

- **SLT**
 - Facilitating training and guidance on Social Media use.
 - Developing and implementing the Social Media policy
 - Taking a lead role in investigating any reported incidents.
 - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required.
 - Receive completed applications for Social Media accounts
 - Approve account creation
- **Administrator/Moderator**
 - Create the account following SLT approval
 - Store account details, including passwords securely
 - Be involved in monitoring and contributing to the account

- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)
- **Staff**
 - Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
 - Attending appropriate training
 - Regularly monitoring, updating and managing content he/she has posted via school accounts
 - Adding an appropriate disclaimer to personal accounts when naming the school

Behaviour

- **The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.**
- **Digital communications by staff must be professional and respectful at all times and in accordance with this policy.** Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with school policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- **Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.**
- **Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.**

Handling abuse

- When acting on behalf of the school, respond to harmful and / or offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken
- If you feel that you or someone else is subject to abuse by colleagues through use of online communications, then this action must be reported using the agreed school protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing online content are:

- Engaging
- Conversational
- Informative
- Professional

We will seek to keep children and young people safe by:

- always asking for written consent from a child and their parents or carers before taking and using a child's image
- always explaining what images will be used for, how they will be stored and what potential risks are associated with sharing images of children

- making it clear that if a child or their family withdraw consent for an image to be shared, it may not be possible to delete images that have already been shared or published
- not using the names of children whose images are being used in our published material whenever possible (and only using first names if we do need to identify them) Names on sports/leavers hoodies will be blurred.
- never publishing personal information about individual children.
- making sure children, their parents and carers understand how images of children will be securely stored and for how long (including how we will control access to the images and their associated information)

Reducing the risk of images being copied and used inappropriately by:

- only using images of children in appropriate clothing
- avoiding full face and body shots of children taking part in activities where there may be a heightened risk of images being misused. We will not take photos of children swimming or in pyjamas.
- using images that positively reflect young people's involvement in the activity.
- images used on social media will only be of the backs of the children's heads, any images of children's faces will be restricted to those with permission and only two photos per post. These photos will be staged by the class teacher and will only include children who have permission. When there is a sporting event, children who do not have permission must wear a coloured bib. Staff will be responsible for checking the permissions list, which is updated by the office manager. The photos will be sent to a member of SLT to be double checked before posting.

We will also develop a procedure for reporting the abuse or misuse of images of children as part of our child protection procedures. We will ensure everyone involved in our organisation knows the procedures to follow to keep children safe.

We use the UK Safer Internet Guidance -

Regularly Review Online Content

We conduct periodic audits of our school's website and social media platforms to assess the necessity of images featuring students. Where possible, we replace identifiable student images with generic school-related visuals.

Apply a 'Names-No-Images / Images-No-Names' Policy

We consider how our school manages images of students and avoid publishing identifiable information/images in publicly accessible materials. For example, by limiting to a first-name only approach, this reduces the likelihood of images being misused or linked to individuals.

Limit Public Visibility of Student Images

Where images of students are necessary, we consider placing them behind a secure, password-protected area, such as a parents' portal.

Ensure Image Metadata is Removed

Before uploading images, we ensure that location data and other metadata (such as EXIF information) have been removed to prevent unintended exposure.

Guide to removing EXIF metadata

EXIF (Exchangeable Image File Format) is a format used to store information (8) (metadata) about something. In relation to images, metadata includes information such as the date and time of when an image was taken, where it was taken and information about the device used.

When uploading such images to public platforms, it is important to ensure that this metadata is removed – whilst some platforms may automatically do this, the following steps are provided as a means to check and remove EXIF data as part of your approach to data security.

PC/Windows

1. Right-click the image file and select Properties and then the Details tab.
2. Click Remove Properties and Personal Information at the bottom of the window
3. Choose from 'Create a copy with all possible properties removed' or 'Remove the following properties from this file'
4. Check the resulting file using Step 1 above to ensure the metadata has been successfully removed

MacOS

1. Open the image in Preview (double-click the image)
2. Click File > Export

3. Under Info, ensure the box 'Include Location Information' is NOT checked
4. Ensure the image title does not contain identifiable information
5. Click Save and then check the resulting file using Step 1 above.

Use Lower Resolution Images

Where images are used, consider reducing their resolution to limit the ability for them to be repurposed.

Strengthen Privacy Settings on School-Managed Platform

We review and apply strict privacy settings (2) to any school-managed social media (3) accounts to control who can access and share posted images. We ensure that approach is in line with any local authority or organisation's social media policy.

Follow Established Image Use Policies

Ensure that all image use aligns with your organisation/local authority data protection policies and that informed consent procedures are in place and up to date. We consider how our approach encompasses the views of C&YP.

Embed Image Security Awareness in Staff Training

We provide regular training to staff on secure image sharing, emerging risks and responsible online content management, including the process to be followed in the event of an incident.

Consider the use of staff imagery in your approach

Our approach addresses how we manage content featuring staff images or videos across the school's online presence.

Engage with Parents and Carers

We maintain open communication with families about how we protect student images and the steps taken to address evolving digital risks. We ensure our safeguarding expectations are clear in relation to images/videos of students being posted on personal social media accounts and why this is important.

Review and ensure effective school policies and processes are in place

Online Safety is a safeguarding issue. Should an incident (4) occur, related safeguarding/child protection policies (5) and procedures should identify clear escalation routes including reporting to the Police and where applicable, the Internet Watch Foundation (6). Ensure all staff are aware of, and understand, their responsibilities.

Work with Trusted Online Safety Partners

Stay informed of best practices and emerging risks by collaborating with organisations such as the UK Safer Internet Centre, SWGfL and the Professionals Online Safety Helpline (7).

4. Photography and/or filming for personal use

When children themselves, parents, carers or spectators are taking photographs or filming at our events and the images are for personal use, we will announce details of our photography policy before the start of the event. This includes:

- reminding parents, carers and children that they need to give consent for Loxwood to take and use their images
- asking for photos taken during the event not to be shared on social media or asking people to gain permission from children, their parents and carers before sharing photographs and videos that include them
- recommending that people check the privacy settings of their social media account to understand who else will be able to view any images they share
- reminding children, parents and carers who they can talk to if they have any concerns about images being shared.

Personal use

- **Staff**
 - Personal communications are those made via a personal online accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
 - Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
 - Where excessive or inappropriate personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
 - *The school permits reasonable and appropriate access to private social media sites.*
- **Learners**
 - **Staff are not permitted to follow or engage with current or prior learners of the school on any personal social media account.**

- The school's education programme should enable the learners to be safe and responsible users of social media.
- Learners are encouraged to comment or post appropriately about the school. Any offensive or inappropriate comments will be resolved by the use of the school's behaviour policy
- **Parents/Carers**
 - **If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.**
 - The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.
 - Parents/Carers are encouraged to comment or post appropriately about the school. In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

Monitoring posts about the school

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

5. If consent is not given

If children, parents and/or carers do not consent to photographs being taken, we will respect their wishes. We will agree in advance how they would like to be identified so the photographer knows not to take pictures of them, and ensure this is done in a way that does not single out the child or make them feel isolated. We will never exclude a child from an activity because we do not have consent to take their photograph.

6. Storing Images

We will store photographs and videos of children securely, in accordance with our safeguarding policy and data protection law. We will keep electronic images in a protected folder with restricted access. Images will be stored for a period of 7 years. We will never store images of children on unencrypted portable equipment such as laptops, memory sticks and mobile phones. Loxwood discourages staff from using any personal equipment to take photos and recordings of children. Only cameras or devices belonging to the Loxwood should be used. Any photos should be downloaded to the google drive and deleted from the device immediately.

7. Links with other policies

This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding and child protection policy and procedures.
- Code of conduct for staff and volunteers.
- Online safety policy and procedures for responding to concerns about online abuse

(1) 360 Safe School Self-Review, Policy & Practice Assessment 2024: <https://swgfl.org.uk/research/england-schools-online-safety-policy-and-practice-assessment-2024>

(2) SWGfL Social Media Checklists: <https://swgfl.org.uk/resources/checklists>

(3) Hwb: Practices and principles for schools' use of social media: <https://hwb.gov.wales/keeping-safe-online/welsh-government-guidance/practices-and-principles-for-schools-use-of-social-media>

(4) UKCIS How to Respond to an Incident (Overview): <https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people>

(5) SWGfL Online Safety Policy Template: <https://swgfl.org.uk/resources/online-safety-policy-templates>

(6) Internet Watch Foundation: <https://www.iwf.org.uk/en/uk-report/>

(7) Professionals Online Safety Helpline: Online Safety support for professionals working with children and young people <https://saferinternet.org.uk/professionals-online-safety-helpline>

(8) Also consider whether any Alt-text (brief descriptions of an image often used to support accessibility) may contain identifiable information.

(9) Third-party tools may offer additional options to further remove EXIF data