# Managing student image and video content

<https://saferinternet.org.uk/guide-and-resource/managing-student-image-and-video-content>

## **Practical actions to take**

**Regularly review online content**

Conduct periodic audits of your school’s website and social media platforms to assess the necessity of images featuring students. Where possible, replace identifiable student images with generic school-related visuals.

* Unsplash: <https://unsplash.com>
* Pexels: <https://www.pexels.com/>
* Pixabay: <https://pixabay.com/>
* Canva: <https://www.canva.com/features/free-stock-photos/>

**Apply a ‘names-no-images / images-no-names’ policy**

Consider how your 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, consider placing them behind a secure, password-protected area, such as a parents’ portal.

**Ensure image metadata is removed**

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

Review and apply strict privacy settings to any school-managed social media accounts to control who can access and share posted images.  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. Consider how your approach encompasses the views of C&YP.

**Embed image security awareness in staff training**

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**

Your approach should address how you manage content featuring staff images or videos across the school’s online presence.

**Engage with parents and carers**

Maintain open communication with families about how the school protects student images and the steps taken to address evolving digital risks.  Ensure your 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 occur, related safeguarding/child protection policies and procedures should identify clear escalation routes including reporting to the Police and where applicable, the Internet Watch Foundation.  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.

* SWGfL Social Media Checklists: <https://swgfl.org.uk/resources/checklists>
* <https://swgfl.org.uk/resources/online-safety-policy-templates>
* <https://saferinternet.org.uk/professionals-online-safety-helpline>