



Maidstone Grammar School
for Girls

Non sibi sed omnibus

Image Use Policy

2026-27

History Log

Last Revised	Revised By	Ratified By Governors	Next Review Date	Time Scale
July 2026	A Swift	30.09.2026	July 2027	Annually

Contact: Mrs A Swift, School Business Manager

A forward-thinking community with a tradition of excellence

Scope and aims of the policy

1. This policy seeks to ensure that images and recordings taken, stored, used or shared by MGGS 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 MGGS community, including parents/carers, staff, governors, 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.
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.
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 MGGS.
5. Images of identifiable individuals are personal data. MGGS 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:
 - o fairly, lawfully and in a transparent manner
 - o for specified, explicit and legitimate purposes
 - o in a way that is adequate, relevant and limited to what is necessary
 - o to ensure it is accurate and up to date
 - o for no longer than is necessary
 - o in a manner that ensures appropriate security
6. The leadership team, supported by the Data Protection Officer (DPO), Designated Safeguarding Lead (DSL) and Governing Body 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

(It is also recognised that staff images may be vulnerable to misuse, impersonation, harassment or manipulation online and so the same safeguarding and proportionality principles apply to staff imagery).

Consent, lawful basis and transparency

7. Consent will not be treated as a one-off administrative process. MGGS will review consent arrangements annually and at key transition points to ensure parents/carers and, where appropriate, child(ren), understand how images may be used. All will be reminded at those times that consent can be withdrawn or amended at any time and all changes will be recorded on a google sheet.
8. Students' 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. Students' 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, MGGS 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'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 admission and annually and reviewed when circumstances change.
14. Where consent is refused, restricted or withdrawn, MGGS will update its records promptly and take reasonable steps to stop further use of the relevant images and remove them from school-controlled platforms where practicable. If there are conflicting views between more than one person who has parental responsibility then the school will treat consent as having not been given for the disputed use.
15. Where people with parental responsibility disagree about image use, or where the position is unclear, MGGS 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.

Safety of images

16. MGGS recognises that images and videos shared online may be copied, downloaded, scraped, altered, manipulated, redistributed or reused without the school'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 MGGS 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 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 student'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 students for personal use.
- use personal devices, personal accounts or personal communication channels to take, store or share images of students.
- display, distribute or publish images unless authorised and the relevant consent or lawful basis has been checked.
- take images of students 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 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.

Images of staff

The school recognises that staff images may be vulnerable to misuse, impersonation, harassment or manipulation online and therefore the same safeguarding and proportionality principles apply to staff imagery.

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 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. MGGS 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. These reviews will be carried out annually in September and recorded by the Designated Safeguarding Lead.

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, 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 children, students with additional needs, or students who may be more vulnerable, particularly where they may be less able to understand or question why images are being taken.
33. MGGS will discuss image use with students 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 students will be selected carefully and will only be used where they are appropriate for the intended purpose.
36. Students will be appropriately dressed in any images used by the school. 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, MGGS will consider whether the image is necessary, proportionate and appropriate for the intended purpose.
39. Where possible, MGGS 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, MGGS will avoid using full names or unnecessary identifying information. In most cases, students 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. MGGS 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, MGGS 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 students and staff images.
43. Where appropriate and proportionate, MGGS 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 students is published or shared publicly, it should be checked by 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.

Use of Video Surveillance, including CCTV

45. 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.

46. 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.
47. MGGS 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.
48. MGGS will identify and document an appropriate lawful basis for using video surveillance and will consider whether a DPIA is required.
49. 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.
50. 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.
51. 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.
52. Recordings will be stored securely, accessed only by authorised individuals and retained only for as long as necessary. The default retention period will be 30 days unless there is a clear reason to retain footage for longer, such as an incident, safeguarding concern, complaint or investigation.
53. 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 images by parents/carers

54. Parents/carers are expected to follow any instructions given by staff before, during or after an event regarding photography or filming. The school may restrict or refuse photography or filming where this is necessary for safeguarding, privacy, dignity, health and safety or operational reasons.
55. Where photographs or videos also include other students, staff, families or visitors, parents/carers are expected not to share these images publicly or upload them to open social media without permission.
56. Parents/carers are not permitted to take photographs or video recordings in sensitive areas of the school, including toilets, changing areas, intimate care areas, swimming areas, sleeping areas or any other area where privacy and dignity may be compromised.
57. Parents/carers are asked not to copy, download, screenshot, redistribute or publicly share images taken or provided by the school unless permission has been given. This includes images shared through websites, social media, newsletters, learning journals, parent/carer platforms or other school systems.
58. Parents/carers who attend activities, trips or events in an official or volunteer capacity are expected to follow the school safeguarding, confidentiality, image use, acceptable use and data protection procedures. This does not prevent parents/carers from taking photographs or videos of their own students for personal and family use where this is permitted by the school. Parents/carers and volunteers should not take photographs or recordings on behalf of the school, or of other students in their volunteer capacity, using personal devices.
59. 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 students

60. MGGS will discuss and agree age-appropriate acceptable use rules with students 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. and the acceptable use of the cameras and/or microphones on their chromebooks.
61. Students will be taught to ask permission before taking images of others and to understand that everyone has the right to say no to being photographed or recorded.
62. Students 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.

63. The use of personal devices by child(ren), including mobile phones, wearable technology, tablets, digital cameras and smart technology, is covered within the school mobile phone and smart technology policy and acceptable use arrangements.
64. Staff will ensure students are appropriately supervised when taking images for official or curriculum use.
65. Images taken by students for official school use will be treated as setting-controlled image use and will be managed in line with this policy.
66. Parents/carers will be informed where students may take images of other students as part of setting-led learning activities, and how these images will be managed.
67. Images taken by students 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

68. Where press or media attendance is planned, MGGS will consider carefully how access will be managed before any photography, filming or interviews take place.
69. Images taken by the press or media may be published more widely than school-controlled images, including online, in print and through social media channels. Once published, the school may have limited control over how images are shared, copied or reused.
70. Appropriate consent will be obtained before students are photographed, filmed or interviewed by the press or media. Where a parent/carer does not give consent, or where a student does not wish to be involved, this will be respected.
71. Particular care will be taken where students, families or staff may be more vulnerable if identified, including students in care, adopted students, students subject to safeguarding plans or court orders, or families affected by domestic abuse, stalking, harassment or other safety concerns.
72. 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 responsibility to manage access to students safely, check consent, consider safeguarding risks and communicate clearly with families.

73. Where press or media attendance is planned, MGGS 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.
74. 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.
75. Unscheduled press or media visits will not be authorised without approval from the Headteacher or other designated senior leader.

Use of external photographers, including videographers and volunteers

76. External photographers engaged to record events or take images on behalf of MGGS must agree to work in line with the school safeguarding, image use, confidentiality and data protection expectations.
77. Where an external photographer processes images on behalf of the school, the school 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.
78. 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.
79. MGGS 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.
80. External photographers will not have unsupervised access to students.
81. Staff, parents/carers or volunteers taking photographs or videos on behalf of the school will be treated as acting in an official capacity and must follow the school safeguarding, confidentiality, image use and data protection expectations. In these

cases, official images will be taken, stored and transferred using school-approved equipment, accounts and systems.

Policy breaches and concerns

82. Members of the school community should report concerns about image use or breaches of this policy in line with existing procedures. This may include reporting to the Headteacher, DSL, DPO or another designated senior leader, and following child protection, data protection, behaviour, complaints, whistleblowing or other relevant procedures.
83. If MGGS 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.
84. The school will prioritise the safety, dignity and emotional wellbeing of any student or adult affected.
85. 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.
86. The school will record the concern and consider whether a safeguarding issue, criminal offence and/or personal data breach has occurred.
87. The school 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.
88. 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.
89. Where threats, blackmail, extortion or suspected criminal activity are involved, the school will seek urgent police and safeguarding advice and will not engage with demands made by individuals attempting to exploit or threaten the school community.
90. The school will consider immediate steps to reduce further access to relevant images. This may include removing images from school-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 students, families and staff.

91. 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.
92. Action will be taken in line with existing school 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.