# NEWLANDS GIRLS' SCHOOL

# POLICY DOCUMENT



# Photographic Images Policy

| LAST UPDATED | Pastoral Deputy Headteacher | March 2024 |
|---|---|---|
| LAST REVIEWED | Pastoral Deputy Headteacher | March 2024 |

| POLICY TYPE | Voluntary |
|---|---|
| REVIEW DATE | Every 3 Years – March 2027 |

| RESPONSIBLE | |
|---|---|
| Leadership Team | Pastoral Deputy Headteacher |
| Governing Committee | Resources Committee |

| APPROVED | |
|---|---|
| Approved By | Full Governing Body |
| Meeting Date | Monday 11th March 2024 |

| UPDATE<br>Shared Drive<br>Website (if applicable) | 19th March 2024<br>19th March 2024 | |
|---|---|---|

# *Courage    Commitment    Compassion*

# PHOTOGRAPHIC IMAGES POLICY

## Aims
At Newlands Girls' School, we use images and videos for a variety of purposes, including prospectuses, display boards, educational purposes, conferences and the school 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.

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.

## Legislation
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
Equality Act 2010
Human Rights Act 1998
Voyeurism (Offences) Act 2019
DfE (2023) 'Keeping children safe in education 2023'

## Roles and Responsibilities
The headteacher is responsible for:
- Submitting consent forms to parents, and pupils where appropriate, at the beginning of the academic year with regard to photos and videos being taken whilst at school.
- Communicating this policy to all the relevant staff members and the wider school community, such as parents.

The DSL/SBM is responsible for:
- Liaising with the DPO 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 photography consent form and requesting any updates or changes via our parent portal
- Acting in accordance with this policy.

## Permissions
We will obtain written consent from parents/carers, or pupils aged 16 and over, for photographs and videos taken of pupils for communication, marketing and promotional materials.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

**Internet/Intranet Sites**
All Parents and Carers sign the Information Technology Acceptable Use Agreement (Appendix 1) when their child joins the school. This states that students should:

*Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.*

**Guidance**
When photographing students:

a. Ensure that the Parents, Carers and pupils (where relevant) have given consent for the material to be used.
b. Ensure all pupils are appropriately dressed.
c. Avoid images that only show a single pupil with no surrounding context of what they are learning or doing. Photographs of three or four students are more likely to also include their learning context.
d. Use photographs that represent the diversity of the young people participating.
e. Do not use images that are likely to cause distress, upset or embarrassment.
f. Report any concerns relating to inappropriate or intrusive photography to the Headteacher.

**Students Photographing Each Other/Trips**

In the case of school trips and offsite activities, the Trip Leader will communicate appropriate protocol to those involved.

**Data Protection**
Photographs and video images of pupils and staff are classified as personal data under the terms of the Data Protection Act 2018.

**Links with other Policies**
- Data Protection Policy with GDPR
- Anti-bullying policy
- Information Technology Acceptable Use Agreement
- Staff Code of Conduct
- Online Safety Policy
- Safeguarding Policy
- Behaviour Policy

# NEWLANDS GIRLS' SCHOOL

## INFORMATION TECHNOLOGY
## ACCEPTABLE USE AGREEMENT - INCLUDING ADVICE TO PARENTS
## (Updated April 2023)

The school uses Information Technology equipment to support the curriculum and help girls extend their learning both inside and outside the classroom. Access to this equipment and these resources is a privilege which, in the event of improper use, can be withdrawn.

*Please read the following sections carefully:*

### Equipment use in school

- Only use the computers for educational purposes

- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the IT equipment.

- If permitted, always check mobile equipment (e.g. laptops, tablet PCs, smartphones etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network. Always check files brought in on removable media (CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses. It is students' responsibility to keep antivirus software up to date.

- Eating and drinking is expressly forbidden in any of the computer rooms, and in any rooms where computer equipment is to be used.

### Security and Privacy

- Your student login details (username and password) are your own personal property and you are responsible for keeping them private and secure. Use them to protect your work and your email account; do not share them with anybody and never use someone else's login.

- Always be wary about revealing any personal information including your home address, telephone number, school name, or picture on the Internet.

- Once logged on, store only your own work on your area; do not store work or files for anybody else, or allow them to store work or files for you.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you, your work, or other girls at risk.

- Computer storage areas will be treated like school lockers. Your computer use may be reviewed by appropriate staff members to ensure that you are using the system appropriately, safely and responsibly.

- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
.
### Internet/Intranet (general advice)

- You should only access the Internet/Intranet for school activities.

- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.

- People you contact on the Internet are not always who they seem. You should never meet with anyone contacted through the internet.

### Email/Messaging (general advice)

- Cyber bullying is dealt with in the same was as any other incident of bullying and is not tolerated at Newlands. Messages sent between students outside school hours still constitute bullying.

- Emails and Teams messages are able to be seen by the IT manager and Leadership Team. You should only send messages that you would be happy for your parents or carers to see.

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.

- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.

- If you receive an email containing material of a violent, dangerous, racist, sexual or inappropriate content, always report such messages to a member of staff/trusted adult **immediately**. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

### Internet advice for Parents/Carers

- Go online with your child and get involved. Search together for useful websites and get to know what Internet resources your child uses. Learn from your child and get to know their online friends.

- Be proactive and caring and warn your child about the dangers of giving out their name, address, telephone number and any other personal information, whether online or not.

- Discuss family and personal values and devise rules for responsible behaviour. Post the rules by the home computer and check to see if they are complied with. At school, teachers will guide pupils on how to use the internet safely. Outside school, families have the responsibility for such guidance.

- Please be aware that if a pupil uses Social Media platforms to harass, cause significant harm to another individual (outside of school hours) or bring the school into disrepute, we may act in school to address such behaviour and/or involve the police when appropriate.

- It is wise to install filtering software and any parental controls that are provided by many commercial online services, but above all else be vigilant.

  Please sign below and once this is returned to school, access to the Internet will be permitted. If a student violates these provisions, access to the Internet will be denied and disciplinary action will be taken. Additional action may be taken by the school in line with existing policy regarding school behaviour. When appropriate, police or local authorities may be involved.

✂...............................................................................................................................................................................................

I have read and support the **INFORMATION TECHNOLOGY - ACCEPTABLE USE AGREEMENT**

Student's Name: _____     Form: _____

Student's Signature: _____

Parent's/Carer's Signature: _____

Date: _____