

# **CHRIST'S HOSPITAL**

## **PHOTOGRAPHY AND VIDEOGRAPHY POLICY**

### **1. Introduction**

Christ's Hospital (CH) is committed to the highest standards of safeguarding and student privacy. To protect the safety and wellbeing of all students, no visitor to Christ's Hospital, including parents and guardians of CH students, is permitted to take photos or videos anywhere on the school site at any time unless specific permission has been granted on a particular occasion.

Only photographers/videographers appointed by and working under contract with Christ's Hospital may take images for approved school purposes. All such activity is strictly controlled through this policy.

For the purposes of this document, the term "photographer" refers to photographers and videographers acting on behalf of Christ's Hospital.

Photographers working on behalf of CH must always respect the rights and privacy of staff, students and visitors.

Images of staff or students may only be used in accordance with the CH Data Privacy Notice. Any use beyond the purposes described in that notice requires explicit consent.

### **2. Appointment of an external photographer**

External photographers may only take images in accordance with a written brief provided by the appointing individual. A contract must be in place governing image creation, storage, use and deletion. A Data Sharing Agreement may be required.

#### **2.1 Image rights and use**

- CH should ideally own all rights to images of school property, staff and students.
- CH involvement must be acknowledged when CH images are used externally.
- CH must be offered the opportunity to support or review any publicity or editorial activity.
- Images of CH, its staff, students or volunteers must not be published, shared or sold in any context that could, in the school's view, damage CH's reputation, misrepresent its ethos or undermine the individuals in the images.
- The photographer must indemnify CH against any legal claims resulting from the recording activity.

#### **2.2 Data sharing requirements**

Data-sharing terms must:

- identify each party's legal status;
- state the lawful basis for image processing;

- define which images will be created and how they will be used;
- set retention periods for staff/student images;
- require immediate deletion of images if consent is withdrawn;
- ensure secure storage in UK GDPR adequacy-approved countries;
- require secure transfer methods;
- set access controls for parent viewing;
- oblige photographers to pass on data subject requests;
- include review and termination provisions.

### **2.3 Supervision and safeguarding**

External photographers must be accompanied by a school host unless cleared under the unescorted contractor process in the Contractors Policy.

### **3. Appointment of an internal photographer**

Internal photographers should only use CH devices. All images captured under a brief are the property of CH.

Internal photographers must:

- store images only within UK GDPR adequacy-approved locations;
- keep images secure at all times;
- transfer images securely to the appointing individual within seven days;
- delete all images from personal devices immediately after transfer.

### **4. Staff capturing images**

Staff may capture images only when this directly supports teaching, learning or other legitimate school purposes.

- Only school-owned devices may be used to capture images of students. Personal devices must not be used under any circumstances.
- Staff must not store student images on personal devices or transfer images to personal accounts or cloud storage.
- Staff must ensure they are aware of, and fully comply with, any students who have withdrawn consent for image use.
- All images must be deleted as soon as they are no longer required, unless they are being retained for clearly defined academic or creative purposes.
- This policy does not prevent staff from taking photographs or videos of their own children who are students at Christ's Hospital. This includes images taken on a personal device, provided that the image features only their own child, is taken for personal use, and is not shared or used in any professional or school-related context.

### **5. Images captured by third party organisations**

During inter-school activities and events, including sports fixtures, performances and joint activities:

- students from Christ's Hospital may be photographed by other organisations as part of the normal course of such events;
- prior to any inter-school activity, CH staff must confirm photography arrangements and permissions with the host organisation. Visiting organisations are expected to do the same when attending events at CH;
- CH photographers may capture action or crowd shots that incidentally include students or staff from other organisations;
- where images include students or staff from another organisation, consent must be obtained from the relevant organisation before any use beyond personal or internal school purposes, including publication or promotional activity;
- requests to use images featuring CH students that have been captured by another organisation must be referred to the Admissions and Marketing Director.

## **6. Visitors (parents, guardians, public)**

Visitors, including parents and guardians, are not permitted to take photos or videos anywhere on the school site at any time unless specific permission has been granted on a particular occasion. This restriction supports safeguarding and student safety; thank you for helping us to keep our students safe.

## **7. Contractors and service providers on site**

Contractors and service providers are not permitted to take photos or videos on the school site unless explicitly authorised in writing by CH for essential operational reasons.

Where authorisation is granted:

- photography must be limited to the contractor's defined work area;
- images must not contain any staff, students, residents, or visitors;
- any image inadvertently capturing a person must be deleted immediately;
- images must not be used for marketing or portfolio purposes;
- images must be stored securely and retained only for the minimum period needed;

## **8. CHEL clients**

CHEL clients, their customers and their guests may take images of buildings and grounds only with prior authorisation. They may not capture images of staff, students or residents.

Commercial images must be approved by the Commercial and Community Access Manager.

All drone use must adhere to CH requirements.

## **9. Drone use**

Anyone operating a drone must be able to demonstrate compliance with the current Drone Code, as applicable:

- You are responsible for flying safely whenever you fly. - Follow the Code.
- Always keep your drone or model aircraft in direct sight and make sure you have a full view of the surrounding airspace.
  - If you fly using first-person view, you must have an observer and follow the rules applicable to use of an observer.
- Fly below 120m (400ft) from the closest point of the earth's surface.
- Do not fly closer to people (not with you) than 50m, including people within structures.
  - You can fly a drone or model aircraft that's below 250g, or UK0, UK1 or C0 class closer to uninvolved people than 50m and you can fly over them.
  - From 1 January 2026 until 31 December 2027, you can also fly a C1 class drone or model aircraft closer to uninvolved people than 50m and you can fly over them.
  - Regardless of a permitted minimum, always keep a safe distance from people.
- Never fly over people who are crowded together.
- Keep at least 150m away from residential, recreational, commercial and industrial areas.
  - You can fly drones and model aircraft that are below 250g, or UK0, UK1 or C0 class in residential, recreational, commercial and industrial areas.
  - From 1 January 2026 until 31 December 2027, you can also do this with a C1 class drone or model aircraft.
- Stay well away from airports, airfields, spaceports and aircraft.
  - If you have a geo-awareness system, it must be up to date.
- Follow any flying restrictions and check for hazards.
- Get the right authorisation if planning to fly outside the code conditions.
- Make sure you know what your drone can and cannot do (operationally).
  - Ensure all functions are set up to operate/not disabled, including any geo-awareness function, and all software is updated.
- Ensure your drone is fit to fly.
  - Check battery and fuel levels, in both the unit and the controller.
- Never drop, lower or fire anything from the drone when it is flying.
- Never carry any dangerous cargo.
- Ensure any equipment attached to the drone is secure.
- Do not fly if the weather could negatively affect flight.
- Ensure you are fit and safe to fly.
- Take action quickly and safely if the situation in the air or on the ground changes.
- Report any dangerous incidents, near misses or suspicious activity.
- Use a flashing green light (on the drone) when flying at night.
- Make sure you have appropriate insurance.
- Respect other people and their privacy.
  - Make sure you know what your camera can do and the kind of images it can take.
  - Make sure you can be clearly seen when flying.
  - Let people know before you start recording or taking pictures.
  - Think before sharing photos and videos.
  - Keep photos and videos secure.
- Always fly safely and legally.
- Label your drone with any required Operator ID.

- Fly with Remote ID switched on if you are flying a UK1, UK2 or UK3 class drone.
- Ensure that anyone who flies your drone has the right competence to do so, such as Flyer ID.
  - Set out what you and they will be responsible for when flying your drone.
- Maintain the drone in a safe flying state.
- You may only fly a drone out of sight if it has follow-me mode capability, set to within 50m of you, and is active.
- If you are asked to observe a tall structure above 105m, you can fly more than 120m above the ground, but no more than 15m above and within 50m of, the structure.

#### General guidelines:

- Fly the same distance away from people horizontally as your height.
- All distances should be increased if the weather is poor.
- All distances should be increased for higher speed flying.
- Do not fly where you could disturb or endanger animals and wildlife.

#### In addition, the following are required as necessary:

- You must have a CAA issued Flyer ID.
  - For drones 100g and above.
  - Your Flyer ID must be current to within five years (renew your Flyer ID).
- You must have an Operator ID.
  - For drones 100g and above with a camera, or drones 250g and above.
  - Your Operator ID must be current to within one year (renew your Operator ID).
- An CAA Operational Authorisation permit if applicable (dependent upon the type of flight to be undertaken):
  - 'Open Category' - A2 flying near people requires an A2 Certificate of Competency.
  - 'Specific Category' flight – Requires CAA Operational Authorisation.
  - 'Certified Category' flight – Requires CAA certification of the aircraft, certification of the operator and licensing of the pilot.
- A risk assessment (RA)
- When the activity will be extensive or complex, a method statement (MS) that incorporates a flight plan.
- A copy of the operator's public liability insurance that provides suitable cover for the planned activity.

The Risk Assessment (and Method Statement) must demonstrate operator compliance with the Drone Code (as a control measure to reduce risk). It must address flight hazards specific to the planned flight area and the potential for a breach of privacy if images of people below or from inside private premises could be captured.

The appointing individual must be satisfied that the RAMS sufficiently address all property, privacy and safety risks. Advice should be sought from the Compliance Manager if there is any doubt about privacy or safety risks. Advice should be sought from the Director of Operations if there is any doubt about property risks. Security must be informed of every flight taking place on the school site in advance.

In the case of a resident, member of staff or student wishing to operate a drone on school premises, approval for the activity must be sought from a Deputy Head. As the appointing individual, the Deputy Head, with the assistance of the Compliance Manager, must ensure Flyer and Operator IDs, Operational Authorisation, RAMS and insurance are in place as appropriate. Ideally the drone operator will have their own public liability insurance, rather than rely on the school public liability or employer's liability insurances which will only be permitted if the activity risk is deemed to be 'low'. A student should only use a drone for academic purposes. A method statement is not always appropriate, but a risk assessment must always be conducted/provided.

Identifiable images of school staff, students and visitors may not be captured by a drone without the express permission of the Admissions and Marketing Director (in writing) in advance of the planned activity. If identifiable images are inadvertently captured, they must be immediately altered so that images are not identifiable or immediately deleted from the recording device. Any request made by the Admissions and Marketing Director to share captured footage with the school must be met.

It is the responsibility of the Admissions and Marketing Director to ensure that, when permission to capture images is given, the lawful reason to do so is set out within the school's Data Privacy Notice. Any new purpose outside of the existing lawful reasons stated in the Privacy Notice must be referred to the Data Protection Officer.

Author: CP/AXP

Date of last review: January 2026

Date of next review: January 2028