

DPIA Data Protection Impact Assessment



The following is reviewed at the start of any major project involving the use of personal data, or if we are making a significant change to an existing process. The final outcomes are integrated back into our project plan.

Submitting controller details

Name of controller	Clarity Independent School
Subject/title of DPO	School Business manager
Name of DPO (delete as appropriate)	Grace Hanson
Title of this DPIA:	CCTV usage
Date of this DPIA review:	April 2026 (reviewed by DPO at the time; Grace Hanson)

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

This project aims to consider both the likelihood and severity of any impact on individuals by use of CCTV and voice recording across the school.

CCTV use across the school is considered by the ICO as a "high risk activity".

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The CCTV video and sound will be continuously operational and capture the events and procedures occurring at the school.

The CCTV system will be managed through the Ring app, which will be password protected and accessible through dual factor authentication. It will be controlled via a single school mobile device which the Head Teacher will keep securely and will be accessible through fingerprint and password security.

All recordings will automatically be deleted after 30 days or kept for the shortest additional time possible until all matters are resolved.

Recordings will not be shared outside the school, except, for statutory requirements such as during an inspection or under safeguarding protocols if necessary. Recordings may be shared with Parents at meetings to share steps of progress.

High Risk – CCTV being continuously operational is considered High risk as it monitors people in school and their workplace, with high probability of some harm or a low probability of serious harm.

Some Harm – infringement of privacy

Serious Harm – Unfair monitoring or decision making.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The CCTV video and sound will be continuously operational and capture the events and procedures occurring at the school to ensure it remains safe. This does not include any special category or criminal data. This also may include capturing parents and visitors to the school.

The school may use the visual and voice recordings captured as part of internal monitoring, for learning observations of the children, for timeline analysis of events, staff training, performance management and for assessments for exam concessions.

The school may also review recordings of meetings and phone calls for the purposes of making accurate, confidential meeting minutes or make written notes from phone calls for our school data communication records.

The school may also voice record students completing activities such as reading, fluency practice exercises or during assessment, to record progress.

All recordings will automatically be deleted after 30 days or kept for the shortest additional time possible until all matters are resolved.

Geographically, the CCTV captures the inside and outside of the school building and playground, alongside the nearest part of the car park outside the school gate.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

As the CCTV video and sound will be continuously operational and capture the events and procedures occurring at the school. This will include surveillance of staff, students, parents and any visitors to the school.

Parents, staff, visitors and students will be aware, as Parents will be asked to sign a Recording, Usage and Retention Consent Form when their child joins the school, staff sign a contract of employment detailing their consent to the use of CCTV at the place of their work, visitors are made aware upon entry to the premises via clear signage and pupils are aware through signage and via parents and teaching staff.

There will visible signs showing that CCTV is in operation displayed at the school gate and access points to the school. Contact details will be displayed on the signs.

Although parents, staff, visitors and students are aware of the use of CCTV, they do not have any control of the data contained therein.

This is considered by the school, to be a usual way to collect and monitor parents, staff, visitors and students' data, in a sensitive setting such as a SEND school, where security and monitoring of vulnerable groups are of paramount importance.

The school has assessed the Ring CCTV system as being safe for this use. It has 3 factor authentication to enter the website app which controls the mobile device controlling the system. The device itself is only accessible through finger-print technology or a 6 digit pin code, by the Head Teacher.

There are no issues of public concern to factor in.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

To promote the health and safety of staff, students and visitors

To enhance the provision of education to our students.

To capture learning observations of the students, monitoring purposes and a timeline analysis of events.

To assist with staff training and performance management.

For assessments for exam concessions.

To review recordings of meetings and phone calls for the purposes of making accurate, confidential meeting minutes or make written notes from phone calls for our school data communication records.

To protect the school buildings and school assets, both during and after school hours.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Discuss infringement of privacy with staff annually when the Photo, Media and CCTV policy is reviewed.

Request that parents complete the Recording, Usage and Retention Consent Form when their child joins the school.

It is not appropriate to consult with Visitors.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimization? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Public Task as the CCTV is being used to enhance the education of the students. It will allow staff to capture learning observations of the students and use this for staff training and then work with students on strategies to progress their learning.

Contract as staff are made aware of the use of CCTV in school before signing their contract. Parents sign the Recording, Usage and Retention Consent Form when their child joins the school.

Legal Obligation as the CCTV assists the school to keep students and employees safe in school.

The has assessed that there is no other way to achieve the same outcome.

This DPIA will be reviewed annually to ensure functions do not creep from their intended purposes.

Individuals are given the information in Step 2.

All data is kept in accordance with the Data Protection Act 2018.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
Privacy infringement for staff as CCTV has voice recording facility. Non-work conversations.	Remote, possible or probable	Minimal, significant or severe	Low, medium or high
Unfair monitoring or decision making against individuals.	Possible	significant	Medium
Counselling sessions for students (CCTV is switched off during these sessions to mitigate risk)	Possible	severe	High
Human Rights violation	Remote	significant	Medium
GDPR infringement (CCTV footage stored securely through Ring App.)	Remote	Minimal	Low
	Remote	significant	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Privacy infringement	Turn off voice recording in staff room.	Eliminated reduced accepted	Low medium high	Yes/no
Unfair monitoring or decision making against individuals.	CCTV only used to formally assess performance management when staff are aware in advance. Use of panels in decision making to avoid bias or unfair outcomes.	Reduced	Low	Yes
Counselling sessions for students	Turn off CCTV camera and sound during sessions.	Eliminated	Low	Yes
GDPR infringement	CCTV footage stored securely through the Ring App accessed by Headteacher only through one device and password protected. Deleted after 30 days or shortest additional time possible until all matters are resolved.	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Debbie Hanson	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Debbie Hanson	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Grace Hanson Business Manager	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: If options in Step 6 are followed this will reduce the risks to an acceptable level.		
DPO advice accepted or overruled by:	Debbie Hanson	If overruled, you must explain your reasons
Comments: N/A		
Consultation responses reviewed by:	N/A	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Grace Hanson	The DPO should also review ongoing compliance with DPIA