

DPIA Report

Account Name

Nelson Academy

DPIA Title

CCTV

Report Date

21/09/26

Identify the need for a DPIA

Need

- ✓ Protect staff, students, visitors and members of the public.
- ✓ Discourage aggressive, abusive and inappropriate behaviour.
- ✓ Protect Nelson Academy's buildings, grounds and infrastructure.
- ✓ Promote a safe community and monitor the security of our premises.
- ✓ Assist in the prevention, investigation and detection of crime.
- ✓ Support the apprehension and prosecution of offenders where appropriate.
- ✓ Provide evidence when investigating incidents, complaints, breaches of policies or codes of conduct involving staff, students or contractors.

Describe the Processing

Nature of Processing

CCTV images and video will be stored on a hard drive unit. Images automatically deleted after 30 days. The source of the data will be pupils, staff, contractors, parents / carers and any other visitor to site.

Data may be shared with police, insurance companies, parents (SAR), staff.

Scope of Processing

Special categories - ethnicity, disability.

Criminal data - theft, trespassing, vandalism, breaking & entering, violent/aggressive acts, inappropriate behaviour.

Data collected remains on the system for 30 days, after which it is automatically deleted.

CCTV covers Nelson Academy site only. It does not cover any private residences.

CCTV operates 24hrs a day.

Any individual who comes onto Nelson Academy's grounds will be affected by the CCTV.

Context of Processing

Visitors

Pupils

Staff

Parents

Contractors

Privacy policies in place explaining how their data is used and stored.

Images will include children and potentially other vulnerable groups.

CCTV system protected by authorised access only and images not visible to passer-by's.

Purpose of Processing

Protect staff, students, visitors and members of the public.

Discourage aggressive, abusive and inappropriate behaviour.

Protect Nelson Academy's buildings, grounds and infrastructure.

Promote a safe community and monitor the security of our premises.

Assist in the prevention, investigation and detection of crime.

Support the apprehension and prosecution of offenders where appropriate.

Provide evidence when investigating incidents, complaints, breaches of policies or codes of conduct involving staff, students or contractors.

Consultation Process

Consultation

Central Trust

Assess Necessity and Proportionality

Necessity

Legal processing - public task.

The data processing does achieve it's purpose.

Function creep - only certain people (role dependant) have access to the CCTV. SLT to authorise whether the task concerned is an appropriate use of retrieving the CCTV data.

CCTV signs located around site, helping parents to locate our website for the policies and guidance, explaining their legal rights and our obligations to protecting their data.

Identify and Assess Risks

Risk	Source of risk and nature of potential impact on individuals	Likelihood of Harm	Severity of Harm	Overall Risk
Insufficient Signage	Invasion of privacy if parents/carers, visitors, staff do not know they are being filmed.	Probable	Significant	Medium

Cyber Attack	Being hacked by an unknown source.	Probable	Severe	High
Unauthorised Access.	Unauthorised access within organisation to CCTV data.	Possible	Significant	High
Individuals unaware of how to exercise their rights over CCTV	Individuals not aware of right to raise a SAR.	Probable	Significant	Medium
Poor maintenance of CCTV	Poor maintenance may lead to systems breaking down and not working effectively.	Possible	Significant	High
Power Outage	Loss of power would mean no data would be recorded. Currently no battery backup.	Probable	Significant	Medium
Failure of Hard Drive	Loss of footage / data - being unable to retrieve data.	Possible	Severe	High

Identify Measures to Reduce Risk

Risk	Risk Measure	Effect on Risk	Residual Risk	Measure Approved
Insufficient Signage	Ensure sufficient signage located on school grounds to make parents/carers, visitors and contractors aware of existence of CCTV. Signage to include information on how to make a data request.	Eliminated	Low	Yes
Cyber Attack	Privacy policy located on website. Systems in operation all protected by firewalls controlled centrally by the Trust.	Eliminated	Low	Yes
Unauthorised Access.	Access only available to authorised personnel via specified mouse. Mouse stored securely. Monitor is not visible to passer-by's due to location and privacy screen attached to monitor to limit visibility to those on the premises.	Reduced	Low	Yes
Individuals unaware of how to exercise their rights over CCTV	Privacy policy available on website. Adequate signage around site leading to privacy and CCTV policy on website.	Eliminated	Low	Yes
Poor maintenance of CCTV	Annual servicing to be carried out on CCTV equipment and any recommended repair works actioned.	Reduced	Low	Yes
Power Outage	Loss of power as a result of	Accepted	Medium	Yes

	bad weather in uncontrollable. Discuss with IT about incorporating a battery back up in case of a power cut.			
Failure of Hard Drive	Annual maintenance carried out on all CCTV equipment and remedial works actioned in a timely manner.	Reduced	Low	Yes

Sign Off and Record Outcomes

Item	Name / Date
Measures Approved by: S	
Date:	
Residual Risks Approved by:	
Date:	
DPO Advice Provided by:	
Summary of DPO Advice:	
DPO Advice Accepted or Overruled by:	
Reasons DPO Overrided:	
Consultation Responses Reviewed by:	
Reasons for departing from views:	
This DPIA will be kept under review by:	