FZ10	Rietveld CCTV Protocol	Version 2.0

Date:	01 July 2012	Revision date:	22 April 2016
Compiled by:	Jan van der Meij	Revision by:	Jan van der Meij

Introduction	Following a series of break-ins, the Gerrit Rietveld Academie decided to install security cameras in December 2010. The cameras are designed to help detect and if possible, prevent theft, vandalism and break-ins.
Privacy	Camera surveillance in the workplace falls under the Personal Data Protection Act (*Wet bescherming persoonsgegevens (Wbp)*). With this protocol, the Gerrit Rietveld Academie aims to safeguard the right to privacy of its students, staff and visitors.
Visibility of cameras	• The cameras shall be placed such that they are visible, aimed at the traffic areas inside and outside the Academie. • In special cases, if there is a suspicion of unlawful actions committed by students or staff, a hidden camera may be temporarily placed. For this, permission must be obtained in advance from the Executive Board/Management Team or the Head of oprations.
Retention period of camera images	• Images of an incident shall be retained until the time this incident has been dealt with, but for not more than four weeks (legal period). • Camera images used in the context of an investigation, which has been reported to the police, shall be destroyed only after consultation with the police. In this case, the legal period of four weeks shall not apply.
Viewing of the images	• The stored camera images shall only be viewed if there is a reason to do so. • Permission for viewing the stored camera images may only be granted by a member of the Executive Board/Management Team or the Head of operations. • The only staff members who are authorised to view the stored camera images are Facility Services staff (Head of Facility Services, Facility Services Coordinator, Head of Facility Implementation, Location Manager), IT (IT Head, Network Administrator) and the IT Administrator (SI). • The images may be viewed by third parties (stakeholders) at the discretion of the Executive Board/Management Team and in the presence of an authorised person. • For controlling access to the premises, real-time camera images (entry barrier, entrance to the new building) shall be viewed from the caretaker's office.
Systems management	• Systems management (IT) staff members are only authorised to install the necessary software and monitor the functioning of the system. The viewing of images shall not be permitted unless explicitly requested by the Head of Facility Services. • Access to the site where the video images are physically stored and access to the option of copying these images shall only be granted to an authorised person (Head of Facility Services, Facility Services Coordinator, Head Caretaker, IT Head, Network Administrator, IT Administrator (SI)).

Information to involved persons	Camera images recording an incident, which has to be reported to the police, may be viewed by the police upon request. The persons involved shall be informed regarding this.
Follow-up	Any irregularity found after viewing the images shall be reported to the client. The Management Team/Executive Board or Head of operations shall determine the follow-up action to be taken.
Questions?	For any questions regarding this policy, please refer to meldpuntFZ@rietveldacademie.nl.