



**ISTITUTO COMPRENSIVO STATALE “DE NICOLA - SASSO”**  
C.so Vittorio Emanuele,77 - 80059 TORRE DEL GRECO (NA)  
Cod. Fisc. 95170080634 - Cod. Mecc. NAIC8CS00C  
Ambito territoriale 21 - Tel./ Fax 081 882 65 00  
[e-mail :naic8cs00c@istruzione.it](mailto:naic8cs00c@istruzione.it) - <http://www.icsdenicolasasso.edu.it>  
PEC: [naic8cs00c@pec.istruzione.it](mailto:naic8cs00c@pec.istruzione.it)  
CERTIFICATA SGQ UNI - EN - ISO 9004:2009

**MUR**  
U.S.R. per la Campania  
Direzione Generale

Polo Qualità di Napoli

# Disciplinare su impiego di sistemi di videosorveglianza negli ambienti dell’Istituto Scolastico “De Nicola-Sasso” – Torre del Greco



# ISTITUTO COMPRENSIVO STATALE "DE NICOLA - SASSO"

C.so Vittorio Emanuele,77 - 80059 TORRE DEL GRECO (NA)

Cod. Fisc. 95170080634 - Cod. Mecc. NAIC8CS00C

Ambito territoriale 21 - Tel./ Fax 081 882 65 00

e-mail :naic8cs00c@istruzione.it - <http://www.icsdenicolasasso.edu.it>

PEC: naic8cs00c@pec.istruzione.it

CERTIFICATA SGQ UNI - EN - ISO 9004:2009

**MUR**  
U.S.R. per la Campania  
Direzione Generale

Polo Qualità di Napoli



**VISTO** il D.lgs n. 196/2003 (codice privacy coordinato con il D.lgs 101/2018) e i principi di liceità, necessità, proporzionalità e finalità in esso sanciti che devono informare ogni trattamento di dati personali;

**VISTO** il "Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio" in materia di trattamento dei dati personali;

**CONSIDERATO** il modello organizzativo privacy adottato dall'ICS De Nicola Sasso e gli atti di designazione delle figure soggettive privacy emanati con Decreto Dirigenziale prot.n. 215/I.4 del 16/01/2023 e con Decreto Dirigenziale prot.n.5727/I.4 del 07/10/2024;

**PRESO ATTO** che il "Disciplinare su impiego di sistemi di videosorveglianza negli ambienti dell'Istituto Scolastico De Nicola - Sasso di Torre del Greco" attiene all'utilizzo dei sistemi di videosorveglianza negli ambienti del citato Istituto ed al trattamento dei dati personali acquisiti attraverso la registrazione delle immagini;

**RILEVATO** che l'installazione di sistemi di videosorveglianza presso gli istituti scolastici deve garantire "il diritto dello studente alla riservatezza" (art.2, comma 2, d.P.R. n. 249/1998) e tenere conto della delicatezza dell'eventuale trattamento di dati relativi a minori;

**VISTO** il Provvedimento del Garante Privacy 8/4/2010 in materia di videosorveglianza;

**VISTE** le Linee guida EDPB 3/2019 sul trattamento dei dati personali attraverso dispositivi video versione 2.0 Adottate il 29 gennaio 2020;

**RITENUTO** fondamentale definire le condizioni e le modalità di corretto utilizzo dei sistemi di videosorveglianza esistenti all'interno dell'Istituto De Nicola - Sasso

**RICHIAMATA** integralmente la delibera del Consiglio di Istituto n. 8 del 10/12/2024 che approva l'istituzione del presente documento quale allegato al Regolamento d'Istituto;

**DECRETA** di emanare il "Disciplinare su impiego di sistemi di videosorveglianza negli ambienti dell'Istituto De Nicola - Sasso".

f.to IL DIRIGENTE SCOLASTICO

Prof. Alessandra Tallarico



## Sommario

Art. 1 - Ambito di applicazione e finalità.....	4
Art. 2 - Definizioni.....	5
Art. 3 - Principi generali.....	7
Art. 4 - Informativa agli utenti.....	8
Art. 6 - Modalità di raccolta dati personali.....	9
Art. 7 - Cancellazione.....	10
Art. 8 - Comunicazione dati.....	10
Art. 9 - Responsabilità, gestione operativa, sicurezza dati.....	10
Art. 10 - Procedura installazione di nuovi impianti, modifica e dismissione degli impianti.....	11
Art. 11 - Procedura di Data Breach negli impianti di videosorveglianza.....	12
Art. 12 - Censimento e manutenzione degli impianti.....	13
Art. 13 - Conformità degli impianti.....	13
ART. 14 - RESPONSABILE.....	13
Art. 15 - Valutazione di impatto (Data Protection Impact Assessment - DPIA).....	14
Art. 16 - Diritti dell'interessato.....	14
Art. 17 - Richieste delle immagini da parte delle autorità.....	15
Art. 18 - Rispetto Statuto dei lavoratori Art. 4 L. 300/70.....	15
Art. 19 - Accertamenti di illeciti e indagini di Autorità Giudiziaria o di Polizia.....	15
Art. 20 - Norma di rinvio.....	16
Art. 21- Efficacia temporale e pubblicità.....	16



## Art. 1 - Ambito di applicazione e finalità

1. Il presente disciplinare si riferisce all'utilizzo di sistemi di videosorveglianza negli ambienti dell'Istituto De Nicola - Sasso di Torre del Greco (di seguito Istituto) ed al trattamento dei dati personali acquisiti attraverso la rilevazione e la registrazione delle immagini.
2. Le immagini sono registrate attraverso l'attivazione di videocamere installate per le finalità istituzionali:
  - a) Prevenire atti vandalici, in modo particolare nelle ore notturne
  - b) Tutelare il patrimonio pubblico da atti vandalici
  - c) Controllare determinate aree esterne al fine di prevenire intrusioni di bulli, disturbatori e venditori ambulanti al fine di garantire la sicurezza e l'incolumità delle persone appartenenti alla comunità scolastica e dei frequentatori degli spazi dell'Istituto nonché di tutelare il patrimonio dell'Istituto.
3. Il sistema di videosorveglianza comporterà esclusivamente il trattamento di dati personali, rilevati mediante le riprese televisive, e che in relazione ai luoghi di installazione delle videocamere, interesseranno i soggetti ed i mezzi di trasporto che transiteranno nell'area interessata.
4. L'attività di videosorveglianza deve raccogliere solo i dati strettamente necessari per il raggiungimento delle finalità perseguitate, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando (quando non indispensabili) immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza. La localizzazione delle telecamere e le modalità di ripresa vanno quindi stabilite in modo conseguente a quanto qui precisato.
5. La possibilità di avere in tempo reale dati ed immagini costituisce uno strumento di prevenzione di atti vandalici ed intrusione di estranei all'interno degli spazi scolastici.
6. L'uso dei dati personali nell'ambito di cui trattasi non necessita del consenso degli interessati in quanto il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento - art. 6 lettera (e).
7. Il trattamento dei dati personali effettuato mediante l'attivazione di impianti di videosorveglianza negli ambienti dell'Istituto, si svolge nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, garantendo la riservatezza, l'identità personale e i diritti degli interessati coinvolti nel trattamento.
8. Le immagini e i dati raccolti tramite gli impianti di videosorveglianza non possono essere utilizzati per finalità diverse da quelle indicate nel presente regolamento e non possono essere diffusi o comunicati a terzi, salvo quanto di seguito disposto o richiesto in caso di indagini di Polizia Giudiziaria.



9. I sistemi impiegati per la videosorveglianza non includeranno componenti che consentano il riconoscimento facciale e/o componenti di I.A. atti a prevenire i comportamenti o elaborare particolari modelli di frequentatori dell'ambiente scolastico.

10. I sistemi di videosorveglianza adottati non dovranno prevedere componenti audio

## Art. 2 – Definizioni

1. Ai fini del presente disciplinare si intende:

- a) per "archivio": qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- b) per "trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- c) per "dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- d) per "misure di sicurezza": il complesso delle misure tecniche, logiche (informatiche), organizzative, fisiche (logistiche e procedurali di sicurezza) che garantiscono il livello adeguato di protezione dei dati personali, previsto dalla normativa vigente;
- e) per "titolare del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; nel caso dell'Istituto il titolare è l'Istituto nel suo complesso;
- f) per "referente interno del trattamento": ai sensi del Decreto di nomina del 16/01/2023 prot.n. 215/I.4. e del Decreto Dirigenziale prot.n. 5727/I.4 del 07/10/2024 I Referenti interni sono così individuati:

Direttore s.g.a - Dott.ssa Carolina Romano

Prof. Giuseppe Romano (Animatore Digitale)



# ISTITUTO COMPRENSIVO STATALE "DE NICOLA - SASSO"

C.so Vittorio Emanuele, 77 - 80059 TORRE DEL GRECO (NA)

Cod. Fisc. 95170080634 - Cod. Mecc. NAIC8CS00C

Ambito territoriale 21 - Tel./ Fax 081 882 65 00

e-mail :naic8cs00c@istruzione.it - <http://www.icsdenicolasasso.edu.it>

PEC: naic8cs00c@pec.istruzione.it

CERTIFICATA SGQ UNI - EN - ISO 9004:2009

**MUR**  
U.S.R. per la Campania  
Direzione Generale

Polo Qualità di Napoli



Ins. Maria Luisa Pentangelo (componente Team dell'innovazione digitale)

Ins. Antonietta Borriello (componente Team dell'innovazione digitale)

Prof.ssa Rita Pernice (componente Team dell'innovazione digitale)

Dott.ssa Marianna De Vito (AA)

Dr. Aldo Ariemma (AA)

- 2) per le strutture amministrative: la/il Direttore/Direttore Generale, per i dati relativi alle proprie attività, e le/i Direttrici/Direttori delle Direzioni per le attività di propria competenza;
- 3) per le strutture di didattica e di ricerca: le/i Direttrici/Direttori dei Dipartimenti e le/i Direttrici/Direttori delle Scuole delle scuole e le/i Direttrici/Direttori dei Centri di 1° livello;
- g) per "autorizzato al trattamento": la persona fisica autorizzata dal responsabile del trattamento a compiere operazioni di trattamento dei dati;
- h) per "referente privacy": figura di supporto al responsabile funzione privacy per agevolare l'attuazione degli adempimenti in materia di protezione dei dati delle persone fisiche, facenti capo al responsabile interno al trattamento dei dati;
- i) per "amministratore di sistema (AdS)": figura professionale individuata nell'ambito informatico, finalizzata alla gestione e alla manutenzione di un 4 impianto di elaborazione o di sue componenti ma anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi;
- j) per "interessato": la persona fisica a cui si riferiscono i dati personali;
- k) per "destinatario": la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali;
- l) per "comunicazione": mettere a conoscenza di dati personali determinati soggetti diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione;
- m) per "diffusione": mettere a conoscenza di dati personali soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione;
- n) per "violazione dei dati personali": la violazione di tipo accidentale o illecito dei dati personali che può consistere nella distruzione, nella perdita, nella modifica, nella divulgazione non autorizzata o nell'accesso ai dati personali trasmessi, conservati o comunque trattati;
- o) per "pseudonimizzazione": il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;



p) per "dato anonimo": il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

q) per "Commissione privacy" un organismo costituito con Decreto Dirigenziale con compiti consultivi e di indirizzo, nonché di analisi dei casi in cui si richiede l'installazione di nuovi impianti di videosorveglianza o di modifica di quelli esistenti. E' composto da: il Presidente della Commissione Privacy D.S. o suo delegato, il Direttore amministrativo DSGA e competente in materia di videosorveglianza o suo delegato, il referente della struttura competente in materia di sistemi informativi e Digitalizzazione o suo delegato in relazione alla natura tecnologica degli apparati di videosorveglianza, eventualmente da un RSPP competente per Aree nei casi in cui si presentino rischi a livello di sicurezza e di tutela della salute, dal responsabile competente in materia di formazione e nei casi in cui l'installazione di impianti possa avere impatti rispetto alla tutela del lavoratore un responsabile delle relazioni sindacali

### Art. 3 - Principi generali

1. La raccolta, la registrazione, la conservazione e in generale l'utilizzo di immagini configurano attività di trattamento di dati personali.

2. Il trattamento di dati personali attraverso sistemi di videosorveglianza da parte dell'Istituto avviene esclusivamente nell'ambito dello svolgimento delle funzioni istituzionali di didattica e ricerca e al fine di garantire la sicurezza e l'incolumità delle persone appartenenti alla comunità scolastica e dei frequentatori degli spazi esterni nonché di tutelare il patrimonio dell'Istituto.

3. I sistemi informatici utilizzati per il trattamento dei dati acquisiti tramite videocamere sono configurati nel rispetto dei principi di privacy by design e privacy by default (Artt. 25 e 5) secondo quanto previsto dal Regolamento UE 2016/679 in materia di protezione dei dati personali.

4. Il trattamento dei dati personali mediante l'attivazione di impianti di videosorveglianza viene effettuato in osservanza dei seguenti principi:

a) principio di liceità: il trattamento dei dati personali è effettuato nell'ambito dell'esercizio di pubblici poteri di cui l'Istituto è investito. In particolare, possono essere attivati sistemi di videosorveglianza solo in quanto strumentali allo svolgimento delle funzioni istituzionali e il relativo trattamento deve avvenire nel rispetto della disciplina in materia di protezione dei dati e di quanto prescritto dalle disposizioni di legge in materia di installazione e utilizzo di apparecchi audiovisivi;

b) principio di necessità: è escluso ogni trattamento superfluo e non correlato alle finalità per cui si è resa necessaria l'acquisizione delle immagini registrate tramite i sistemi di videosorveglianza installati negli ambienti dell'Istituto;

c) principio di proporzionalità: l'installazione di impianti di videosorveglianza negli ambienti dell'Istituto si basa su una ponderata valutazione che tenga conto dell'insufficienza e/o della difficoltà di attivare altre misure utili agli scopi connessi all'esercizio dei pubblici poteri.



#### Art. 4 - Informativa agli utenti

1. In ottemperanza a quanto disposto dalla normativa in materia, in prossimità delle postazioni in cui sono installate le apparecchiature per la videosorveglianza, deve essere affissa adeguata segnaletica permanente sulla base del facsimile di “informativa semplificata” riportata nelle linee guida EDPB in vigore dal gennaio 2020 in materia di videosorveglianza. Tale informativa semplificata o minima deve contenere almeno l’indicazione del titolare del trattamento, delle finalità del trattamento, modalità di ripresa, durata di conservazione delle immagini, diritti degli interessati, dati di contatto e un collegamento telematico all’informativa estesa.
2. Il supporto segnaletico elaborato secondo lo standard uniforme dell’Istituto (vedi allegato)
  - deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
  - deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
  - può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.
3. In presenza di più telecamere, in relazione alla vastità dell’area oggetto di rilevamento e alle modalità delle riprese, potranno essere installati più supporti segnaletici.
4. Qualora l’impianto sia in funzione anche in orario notturno, l’informativa deve essere visibile.
5. Il soggetto designato cura il monitoraggio relativo all’affissione, alla regolarità ed alla manutenzione dei supporti segnaletici contenenti l’informativa semplificata e provvede, con il supporto del referente competente per i sistemi informativi a fornire, in modo facilmente accessibile anche con strumenti informatici e telematici, in particolare, tramite reti Intranet o siti Internet, affissioni in bacheche o locali, avvisi e cartelli agli sportelli per gli utenti, , l’informativa privacy estesa contenente le informazioni specifiche e complete secondo quanto previsto dall’art.13 del Regolamento UE 2016/679.

#### Art. 5 – Conservazione dei dati

1. Le immagini registrate sono conservate, ordinariamente, per un periodo di 24 ore dalla rilevazione, fatte salve specifiche esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici e servizi, calendario delle lezioni, in ogni caso non possono essere conservate per un periodo superiore alla settimana (7 giorni pari a 168 ore) nel rispetto delle prescrizioni del Provvedimento generale del Garante per la protezione dei dati personali in materia di videosorveglianza del 2010 e successive modifiche. Quanto più prolungato è il periodo di



conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l'analisi riferita alla legittimità dello scopo e alla necessità della conservazione.

2. L'Istituto, nella persona del Dirigente Scolastico, sentito la Commissione Privacy per i profili del rispetto di principi privacy by design, privacy by default, minimizzazione dei dati e delle linee guida dei Garanti europei in materia di valutazione di impatto privacy (art. 15 del presente regolamento), può stabilire, con provvedimento motivato di conservare le immagini per un periodo più ampio nel caso di specifiche e documentate esigenze tecniche connesse al livello di rischiosità dell'attività svolta e facente capo al titolare del trattamento, nonché su richiesta dell'Autorità Giudiziaria o delle Forze di Polizia, ovvero per attività difensive a tutela dell'ente e della comunità scolastica.

#### Art. 6 - Modalità di raccolta dati personali

1. I dati personali sono acquisiti attraverso impianti di videosorveglianza per l'attivazione dei quali deve essere garantita la conformità a misure di sicurezza informatiche e organizzative adeguate, previste dalle normative vigenti e dalle policies dell'Istituto in materia di sicurezza informatica.

2. I soggetti che svolgono attività di installazione, manutenzione e gestione degli impianti e che visualizzano le immagini, sono designati come Responsabili del trattamento dei dati personali, ai sensi degli art. 28 del Regolamento U.E. 2016/679 in materia di protezione dei dati o come soggetti autorizzati dal D. S. in qualità di titolare del trattamento. Gli autorizzati sono tenuti a seguire corsi di formazione e aggiornamento e sono vincolati ad accordi di riservatezza per la tutela dei dati, delle informazioni e dei documenti di cui siano venuti a conoscenza nell'espletamento delle attività.

3. Il titolare del trattamento fornisce, per iscritto alle persone autorizzate, le istruzioni relative al trattamento e alla conservazione dei dati, alla loro protezione contro eventuali rischi di violazione. Tali istruzioni sono condivise con il referente per i sistemi informativi in relazione ai profili tecnologici e informatizzati del trattamento e sono aggiornate in caso di modifiche tecniche, normative e organizzative. Il DSGA conserva, nel rispetto del principio di accountability, tutta la relativa documentazione.

4. Il D.S. definisce i profili di abilitazione per l'accesso alle immagini tramite sistemi automatizzati e autorizza l'accesso fisico alle sale di controllo, consentito esclusivamente, in via ordinaria, al referente dei sistemi informativi, il personale adeguatamente istruito sui livelli di sicurezza, alla ditta manutentrice dell'impianto all'uopo designato come Responsabile del trattamento dei dati personali assistito dal personale dell'Istituto, fermo restando l'accesso consentito alla polizia giudiziaria, nei casi espressamente previsti per motivi di ordine pubblico, sicurezza, tutela del patrimonio e repressione dei reati.



5. L'accesso di soggetti diversi da quelli indicati può avvenire solo in via eccezionale per comprovata e documentata necessità in relazione alle finalità sopra indicate, previa autorizzazione del DSGA. Le immagini sono conservate su appositi server o supporti analogici custoditi nel rispetto delle misure di sicurezza richieste dalla normativa vigente e delle policies di sicurezza informatica definite dalla Commissione privacy.

#### Art. 7 – Cancellazione

1. Le immagini registrate vengono cancellate automaticamente da ogni supporto allo scadere del termine di conservazione stabilito ai sensi dell'art. 5 del presente disciplinare con sovraccarico di registrazioni e modalità che rendano non più disponibili in modo irreversibile i dati cancellati.

#### Art. 8 - Comunicazione dati

1. La comunicazione e la diffusione delle immagini raccolte presso i plessi dell'Istituto è prevista dalla legge nei casi in cui ne facciano richiesta le forze di polizia e l'autorità giudiziaria per finalità di difesa e sicurezza dello Stato o di prevenzione, accertamento e repressione di reati. La comunicazione e la diffusione verso organismi di informazione sono vietate salvo casi eccezionali e in tal caso devono essere autorizzate per iscritto dal Dirigente Scolastico consultato la commissione privacy.

2. Non si considera comunicazione, ai sensi e per gli effetti del precedente comma, la conoscenza dei dati personali riferiti alle immagini da parte delle persone autorizzate per iscritto dal titolare o dal responsabile a compiere le operazioni del trattamento.

#### Art. 9 - Responsabilità, gestione operativa, sicurezza dati

1. Il Dirigente Scolastico per il tramite del soggetto designato del trattamento è tenuto a:

- nominare con atto scritto gli autorizzati del trattamento;
- vigilare sulla conservazione delle immagini e sulla loro cancellazione al termine del periodo previsto per la conservazione delle stesse;
- presidiare con funzioni di responsabilità il procedimento volto all'esercizio del diritto di accesso ai dati da parte dell'interessato e/o delle autorità competenti;
- redigere e aggiornare la scheda di censimento relativa al trattamento connesso alla videosorveglianza ai fini del registro dei trattamenti;
- monitorare ed aggiornare il censimento annuale relativo alla mappatura degli impianti;
- vigilare sulla manutenzione e il buon funzionamento degli impianti e redige una relazione periodica in materia;
- presidiare il monitoraggio dell'informatica semplificata tramite cartellonistica per la segnalazione della presenza di telecamere e delle informative privacy per esteso, documentare tutte le attività con verbali e report ed effettuare, in sinergia con il referente



privacy competente per i sistemi informativi, l'analisi del rischio e nei casi previsti anche la valutazione di impatto prevista dall'art. 35 del regolamento privacy;

h) verificare, con specifici audit, le misure per garantire l'integrità e la disponibilità dei dati e i criteri e le modalità di ripristino dei dati.

2. Il Titolare designa referenti di Plesso di supporto con il compito di agevolare gli adempimenti e il raccordo con Il Responsabile per la protezione dei dati personali e gli utenti.

3. Il Dirigente scolastico designa e nomina gli incaricati al trattamento dei dati personali assegnando compiti specifici seguite da dettagliate istruzioni in ordine all'utilizzo dei sistemi e delle immagini in diretta provenienti dalle videocamere. A tali immagini possono accedere soltanto i collaboratori scolastici nominati incaricati al trattamento dei dati di videosorveglianza che prestano servizio nella postazione di controllo dell'accesso principale dell'Istituto

#### Art. 10 - Procedura installazione di nuovi impianti, modifica e dismissione degli impianti

1. I referenti di plesso che intendono installare nuovi impianti sono tenuti a contattare la Direzione dell'Istituto, a consultare la specifica documentazione in materia di videosorveglianza, con il supporto del proprio referente privacy di struttura, alla sopracitata Direzione e al referente privacy competente in materia di sistemi informativi, la specifica richiesta nella quale occorre specificare: finalità, tipologia di impianto, luogo di installazione.

2. La Commissione privacy formula un parere tecnico di indirizzo e si esprime sulla base della documentazione ricevuta in merito alla fattibilità, alla sostenibilità dell'installazione, alla valutazione della strumentazione tecnologica più idonea in base alle finalità indicate e alle specifiche tecniche richieste alla luce delle policies di sicurezza dell'Istituto ed esamina ove richiesta la DPIA prodotta dal Referente privacy competente per i sistemi informativi.

3. Qualora la scelta tecnologica o il tipo di impianto da installare al vaglio della Commissione presenti elementi di forte criticità dal punto di vista della Protezione dei Dati Personal, è necessario informare il Responsabile per la protezione dati dell'Istituto in merito ai punti di attenzione rilevati e richiedere allo stesso un parere sulla conformità in materia di protezione dati.

4. La Commissione privacy documenta il processo in un verbale che deve essere tenuto agli atti.

5. Nel caso di valutazione positiva, la Commissione contatta il referente del plesso richiedente per l'implementazione dell'impianto, fornendo le linee di indirizzo.

6. Il referente privacy competente per i sistemi informativi predispone e propone l'analisi dei rischi alla Commissione privacy per una sua valutazione del rischio connesso al trattamento delle immagini, per la tutela dei diritti e delle libertà degli interessati. La stessa Direzione qualora ne ravvisi la necessità può richiedere informazioni aggiuntive al referente del plesso che ha presentato domanda di installazione.



7. La Direzione Amministrativa (DSGA) è responsabile del procedimento di installazione ed è tenuta a verbalizzarne le operazioni.
8. Nel caso in cui fossero riprese postazioni di lavoro, la Commissione privacy coinvolge il Direttore Amministrativo competente per i rapporti in materia di personale per gli adempimenti connessi alle relazioni sindacali come previsto dall'art. 4 dello Statuto dei lavoratori.
9. Nel caso di richieste di modifica dell'impianto di videosorveglianza (angolo di visuale, periodo di conservazione, caratteristiche tecniche) viene inviata la richiesta dal referente di plesso e presa in carico da parte del Dirigente Amministrativo che può coinvolgere eventualmente, per gli aspetti legati ai sistemi informatici il referente competente per i sistemi informativi.
10. La Direzione amministrativa (DSGA) istruisce la pratica per verificare la conformità delle installazioni e delle modifiche proposte, dispone sopralluoghi, relaziona per iscritto la Commissione privacy e fornisce le planimetrie con indicazione della scala utilizzata nella rappresentazione del diagramma o progetto.
11. Nel caso di richiesta di dismissione corredata dalle relative motivazioni, la Direzione amministrativa istruisce la pratica e informa la Commissione privacy;
12. A seguito dell'istruttoria e sulla base delle indicazioni della Commissione privacy che ha rilasciato una valutazione positiva per la nuova installazione o la modifica di impianti di videosorveglianza informatizzati, il referente privacy competente per i sistemi informativi attiva tutte le procedure tecniche contenute nelle policies di sicurezza informatica con particolare attenzione a: - distruzione delle immagini, durata di conservazione dei log, cancellazione dei log e degli accessi ai dati; cancellazione degli eventuali backup.
13. La Direzione amministrativa aggiorna la documentazione nei casi di modifica e dismissione degli impianti.
14. Le procedure di modifica e dismissione di impianti possono essere attivate d'ufficio da parte della Direzione amministrativa per motivi di costi, obsolescenza e sicurezza, previa acquisizione parere della Commissione privacy.

#### Art. 11 - Procedura di Data Breach negli impianti di videosorveglianza

1. Nel caso di violazione di dati: perdita, distruzione, alterazione delle immagini o di incidente informatico relativo agli impianti di videosorveglianza con impatto sui dati, occorre attivare la procedura dell'Istituto Data Breach, entro 72 ore dall'avvenuto accertamento della violazione. Qualora l'impianto di videosorveglianza tratti dati biometrici, la notifica all'Autorità Garante deve essere inviata entro 48 ore dall'avvenuto accertamento della violazione, secondo quanto previsto dal Provvedimento generale dell'Autorità Garante in materia.
2. La decorrenza di tali limiti temporali scatta secondo i criteri stabiliti dalla procedura di Data Breach dell'Istituto.



3. I criteri temporali definiti al comma 1 del presente articolo, dovranno essere aggiornati qualora la normativa di settore lo richieda o a seguito di interventi puntuali dell'Autorità Garante.

### Art. 12 – Censimento e manutenzione degli impianti

1. La Direzione amministrativa e il referente privacy competente per i sistemi informativi, ciascun per le rispettive competenze, sono tenuti a monitorare periodicamente gli impianti di videosorveglianza, e gli apparati informatici relativi alla raccolta e all'archiviazione delle immagini, per verificare la funzionalità tecnica avendo anche cura che la cartellonistica fornita sia aggiornata e per intervenire con opere di manutenzione ordinaria e straordinaria.
2. La Direzione amministrativa cura periodicamente l'aggiornamento del censimento degli impianti identificati con relativa numerazione univoca progressiva e provvede all'aggiornamento del registro dei trattamenti dei dati.

### Art. 13 - Conformità degli impianti

1. Il settore competente della Direzione amministrativa che si occuperà dell'acquisto del materiale per videosorveglianza deve verificare e garantire che vengano fornite le specifiche attestazioni e certificazioni tecniche nel rispetto dei principi privacy by default e privacy by design e in conformità al Regolamento UE 2016/679.
2. Qualora ne ricorrono i presupposti, la Direzione amministrativa - è tenuta a perfezionare e fare siglare all'azienda manutrice l'accordo di designazione a responsabile esterno al trattamento.

### ART. 14 - RESPONSABILE.

1. La ditta manutrice, è individuata quale responsabile del trattamento dei dati personali rilevati, ai sensi e per gli effetti dell'art.28 del Reg. U.E. 2016/679.
2. Il responsabile deve rispettare pienamente quanto previsto, in tema di trattamento dei dati personali, dalla normativa positiva, ivi incluso il profilo della sicurezza, e dalle disposizioni del presente disciplinare.
3. Il responsabile procede al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sull'utilizzo dei sistemi e sul trattamento delle immagini e dei dati, in conformità agli scopi perseguiti dall'Istituto, ed alle altre disposizioni normative che disciplinano la materia ed in particolare alle eventuali disposizioni impartite dall'Autorità Garante per la protezione dei dati personali, nonché sulla puntuale osservanza delle disposizioni di cui al comma i e delle proprie istruzioni.
4. I compiti affidati al responsabile devono essere analiticamente specificati per iscritto, in sede di designazione.
5. Il Responsabile nominerà gli incaricati del materiale trattamento dei dati nei limiti che saranno ivi specificati. Gli incaricati devono trattare i dati personali ai quali hanno accesso attenendosi scrupolosamente alle limitazioni previste nell'atto di nomina ed alle eventuali



istruzioni del responsabile.  
 6. Il Responsabile, qualora incaricato, custodisce le chiavi dell'armadio destinato alla conservazione delle registrazioni nonché le parole chiavi per l'utilizzo del sistema.

#### Art. 15 – Valutazione di impatto (Data Protection Impact Assessment - DPIA)

1. Nei casi in cui dall'analisi del rischio effettuata risulti un livello di rischio elevato, il referente privacy competente per i sistemi informativi e la Direzione amministrativa procedono a effettuare la Data Protection Impact Assessment - DPIA o Valutazione di Impatto in ambito Protezione Dati Personalni coinvolgendo le funzioni interessate.
2. La valutazione di impatto è richiesta nei casi previsti dall'art. 35 del Regolamento UE 2016/679; dalle linee guida del Comitato Europeo per la Protezione dei dati personali (ex Gruppo di lavoro art. 29) e dai provvedimenti dell'Autorità Garante.
3. Il referente privacy competente per i sistemi informativi e la Direzione amministrativa elaborano una specifica metodologia in materia di DPIA che sarà sottoposta alla Commissione privacy.
4. Il Responsabile per la protezione dei dati personali è tenuto a fornire, se richiesto dal Titolare, un parere in merito alla valutazione d'impatto sulla protezione dei dati ai sensi del citato articolo 35.

#### Art. 16 - Diritti dell'interessato

1. L'interessato, dietro presentazione di apposita istanza, potrà rivolgersi al Direttore amministrativo, quale Responsabile del procedimento del trattamento dati di videosorveglianza al fine di:
  - a) ottenere conferma circa l'esistenza di trattamenti di dati/immagini che possano riguardarlo;
  - b) essere informato sugli estremi identificativi del titolare e del responsabile oltre che sulle finalità e le modalità del trattamento cui sono sottoposti i dati;
  - c) opporsi, indicandone il motivo, in tutto o in parte al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta.
2. Le istanze di cui al presente articolo devono essere protocollate.
3. La Direzione amministrativa è tenuta a informare in merito al ricevimento delle istanze di esercizio dei diritti, il Responsabile per la protezione dei dati personali, fornire un documentato riscontro (con nota protocollata) entro 30 giorni, tenere e aggiornare un registro delle istanze sulle immagini.
4. La Direzione amministrativa pubblica il facsimile per la presentazione delle istanze di esercizio dei diritti sui dati e fornisce agli interessati informazioni e supporto sulle relative modalità.



### Art. 17 – Richieste delle immagini da parte delle autorità

1. Nel caso di richiesta delle immagini da parte della Polizia Giudiziaria, della Polizia Postale, ogni funzione coinvolta è tenuta a fornire prontamente massima disponibilità e collaborazione e nei casi in cui sia possibile e sostenibile è tenuta ad avvertire immediatamente: il Dirigente scolastico, la Direzione amministrativa, il referente privacy competente per i sistemi informativi, il settore competente in materia di personale , la Commissione privacy e il Responsabile della protezione dei dati personali.
2. Viene documentata attraverso specifico verbale ogni attività sulle immagini richieste dall'Autorità. Viene aggiornato il dedicato registro delle richieste dei diritti degli interessati.
3. Le registrazioni sono messe a disposizione dell'Autorità Giudiziaria o di altre pubbliche Autorità solo in presenza di provvedimenti da queste emanati.

### Art. 18 – Rispetto Statuto dei lavoratori Art. 4 L. 300/70

1. Nei casi in cui derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, (riprese delle postazioni di lavoro o dei lavoratori nello svolgimento delle loro mansioni), gli impianti di videosorveglianza, possono essere installati nel rispetto di quanto previsto dall'art. 4 dello Statuto dei Lavoratori esclusivamente per finalità motivate da esigenze organizzative e produttive, da motivi di sicurezza del lavoro e di tutela del patrimonio aziendale, solo previo accordo con le rappresentanze sindacali unitarie dell'Istituto. Nel caso di mancato accordo con le rappresentanze sindacali, l'Istituto si avvale, nei termini di legge, dell'autorizzazione della Direzione Territoriale dell'Ispettorato del Lavoro.
2. Qualora in riferimento ad impianti di videosorveglianza già installati, vi siano segnalazioni che evidenziano la possibilità di controllo a distanza dell'attività dei lavoratori, il responsabile del plesso interessato e/o le rappresentanze sindacali unitarie ne danno comunicazione scritta al Commissione privacy ed al Responsabile per la Protezione dati dei dati. Qualora si rendano necessari aggiornamenti e/o modifiche significative all'impianto di videosorveglianza il Dirigente Scolastico convoca uno specifico incontro ove le parti coinvolte valutano l'opportunità di redigere un nuovo verbale di accordo sindacale e nel caso ne ricorrono le motivazioni predisporre le correlate informative ai sensi dell'art. 13.

### Art. 19 – Accertamenti di illeciti e indagini di Autorità Giudiziaria o di Polizia

Ove dovessero essere rilevate immagini di fatti che possano portare a ipotesi di reato o di eventi rilevanti ai fini della sicurezza pubblica, l'incaricato della videosorveglianza né darà immediata comunicazione al Dirigente Scolastico per le valutazioni del caso. In tali casi, in deroga alla puntuale prescrizione delle modalità di ripresa, l'incaricato potrà procedere agli ingrandimenti della ripresa delle immagini strettamente necessari e non eccedenti allo specifico scopo perseguito.



## ISTITUTO COMPRENSIVO STATALE "DE NICOLA - SASSO"

C.so Vittorio Emanuele, 77 - 80059 TORRE DEL GRECO (NA)

Cod. Fisc. 95170080634 - Cod. Mecc. NAIC8CS00C

Ambito territoriale 21 - Tel./ Fax 081 882 65 00

e-mail :naic8cs00c@istruzione.it - <http://www.icsdenicolasasso.edu.it>

PEC: naic8cs00c@pec.istruzione.it

CERTIFICATA SGQ UNI - EN - ISO 9004:2009

**MUR**  
U.S.R. per la Campania  
Direzione Generale

Polo Qualità di Napoli

Alle informazioni raccolte ai sensi del presente articolo possono accedere solo gli organi di Polizia e l'Autorità Giudiziaria. L'apparato potrà essere utilizzato anche in relazione ad indagini di Autorità Giudiziaria o di organi di Polizia.

Le registrazioni sono messe a disposizione dell'Autorità Giudiziaria o di altre pubbliche Autorità solo in presenza di provvedimenti da queste emanati.

### Art. 20 - Norma di rinvio

1. Per quanto non previsto dal presente Regolamento, si applicano le disposizioni previste dal Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 e dal Regolamento dell'Istituto in materia di protezione dati personali.

### Art. 21- Efficacia temporale e pubblicità

1. Il presente Disciplinare entra in vigore a partire dal 11/12/2024 per gli impianti di nuova installazione e per i "principi generali" di cui all'art. 3. Per gli impianti in essere e per le modifiche all'attuale configurazione degli impianti già installati alla data di approvazione del disciplinare, il medesimo entrerà in vigore dal 11/12/2024, nell'ipotesi che sia concluso il censimento tecnico e gestionale degli impianti. L'Istituto provvede a dare pubblicità al presente Disciplinare ed alle successive modifiche ed integrazioni mediante comunicazione e pubblicazione nei modi d'uso dell'Istituto.