ISTITUTO DI ISTRUZIONE SECONDARIA SUPERIORE STATALE "EMILIO SERENI"
AFRAGOLA – CARDITO

Regolamento

per l'installazione e l'utilizzo del sistema di videosorveglianza all' interno dell' istituzione scolastica

Introduzione e ambito di applicazione

Il presente REGOLAMENTO disciplina e documenta l'esercizio del "Sistema di Videosorveglianza" gestito presso l'ISIS SERENI AFRAGOLA – CARDITO in conformità al D.Lgs.. 196/03, nonché, in modo più specifico, il Provvedimento in materia di videosorveglianza del Garante datato 8 aprile 2010 e pubblicato sulla Gazzetta Ufficiale n. 99 del 29 aprile 2010, come anche il Parere 2/2009 sulla "Protezione dei dati personali dei minori (Principi generali e caso specifico delle scuole)", adottato l'11 febbraio 2009 dal Gruppo di Lavoro articolo 29 sulla protezione dei dati personali, e nella guida del Garante della Privacy "La privacy tra i banchi di scuola", ove è contenuto un apposito paragrafo dedicato alla videosorveglianza; unitamente all'art. 2, comma 2, del D.P.R. n. 249/1998, che, nel riconoscere esplicitamente "il diritto dello studente alla riservatezza", obbliga a tenere conto di tale diritto quando si affronta l'eventuale installazione di un impianto di videosorveglianza.

Le finalità che l'ISS "E.Sereni" intende perseguire con la videosorveglianza sono quelle rispondenti ad alcune delle funzioni istituzionali che fanno capo alla responsabilità dell'Istituto quali il controllo e la sorveglianza degli accessi e la prevenzione di furti e di atti vandalici, atti e comportamenti lesivi dell'altrui incolumità e di prevenzione di atti di bullismo.

La disponibilità tempestiva di immagini costituisce uno strumento di prevenzione e di razionalizzazione dell'azione e degli interventi dei Collaboratori scolastici, dei docenti, degli organi quali cdc, vicepresidenza , dirigenza.

L'impianto di videosorveglianza, in sintesi, è finalizzato:

1. **ad assicurare maggiore sicurezza agli studenti e agli operatori scolastici;**
2. **a tutelare il patrimonio da atti vandalici;**
3. **al controllo di determinate aree all'aperto non presidiate**.

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali. È considerato dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

Il sistema di videosorveglianza impiegato presso l'Istituto è gestito nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare rifermento alla tutela dei dati personali. Inoltre, la sua installazione garantisce il diritto dello studente alla riservatezza. Sono altresì garantiti i diritti delle persone giuridiche e di ogni altro ente o associazione coinvolti nel trattamento dei dati rilevati e acquisiti tramite le registrazioni.

Il sistema è stato installato seguendo il principio di necessità, mediante un'attenta configurazione del sistema informativo e dei programmi informatici, col fine di ridurre al minimo l'utilizzazione di dati personali, prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione e al loro diritto all'educazione.

Visto che il Garante della privacy ha previsto che è ammessa l'installazione di telecamere per la tutela contro gli atti vandalici, ***il servizio di videosorveglianza dell' Isis Sereni Afragola-Cardito funzionerà per l'intera giornata.***

Considerato che nell' ISTITUTO SERENI AFRAGOLA-CARDITO , è stato progettato e collaudato un impianto di videosorveglianza, per il quale, nel rispetto della normativa, occorre procedere alla stesura del Regolamento, il Dirigente scolastico Dott.ssa Daniela Costanzo

Emana

il seguente "**Regolamento per la videosorveglianza**" che verrà pubblicato sul sito web della scuola ed all'albo della sede dell'Istituto.

TITOLO I — Descrizione

Art. 1. Definizioni specifiche

1. Videosorveglianza: sistema o dispositivo che permette la visione e la registrazione su supporti singoli, abbinati ad altre fonti o conservati in banche di dati di immagini di aree o zone delimitate;

2. Centrale di Videosorveglianza: sistema centrale dove sono convogliate ed eventualmente registrate tutte le riprese effettuate dai dispositivi periferici.

Art. 2. Definizioni D.Lgs. n.196/03.

1. Trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.
2. Dato personale: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
3. Dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato.
4. Dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazi oni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
5. Dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
6. Titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
7. Responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
8. Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.
9. Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.
10. Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato (dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati), in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

11. Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
12. Dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
13. Blocco: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.
14. Banca di dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.
15. Garante: l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675;
16. Comunicazione elettronica: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.
17. Reti di comunicazione elettronica: i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato.
18. Rete pubblica di comunicazioni: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico.
19. Servizio di comunicazione elettronica: i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio del 7 marzo 2002.
20. Dati relativi all'ubicazione: ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico.
21. Misure minime: il complesso delle misure tecniche, informatiche, organizzative, logistiche procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

22. Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.
23. Sistema Informativo: l'insieme di dispositivi, programmi ed infrastruttura di rete.
24. Autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.
25. Credenziali di autenticazione: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
26. Parola chiave: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.
27. Profilo di autorizzazione: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
28. Sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati.

TITOLO II – Principi e Finalità

Art. 3. Principio di Liceità.

1. Ai Sensi del D.Lgs. n.196/03 (Codice Privacy), l'ISIS SERENI AFRAGOLA-CARDITO effettua il trattamento dei dati attraverso sistemi di videosorveglianza per la tutela dell'edificio e dei beni scolastici esclusivamente negli orari di chiusura dell'Istituto.
2. l'ISIS SERENI AFRAGOLA-CARDITO si riserva altresì di trattare i dati tramite sistemi di videosorveglianza, quale misura complementare ai fini della Tutela della sicurezza all'interno e all'esterno delle singole strutture.
3. La videosorveglianza avverrà nel rispetto, oltre che della disciplina di protezione dei dati, di quanto prescritto dalle vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela ed infine dalle norme del codice penale che vietano le intercettazioni di comunicazioni e conversazioni.
4. l'ISIS SERENI AFRAGOLA-CARDITO effettuerà il trattamento dei dati attraverso sistemi di videosorveglianza tenendo presenti le norme riguardanti la tutela dei lavoratori ai sensi della Legge n. 300/1970.

Art. 4. Principio di Necessità.

1. Al trattamento dei dati attraverso sistemi di Videosorveglianza è applicato il principio di necessità, pertanto qualsiasi trattamento non conforme a questo principio è da ritenersi illecito (artt. 3 e 11, comma 1, lett. A), del Codice Privacy

2. Il sistema a supporto degli impianti di Videosorveglianza sono conformati in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi
3. L'impianto di Videosorveglianza è conformato in modo da non permettere l'identificazione dell'interessato
4. L'eventuale registrazione di dati personali non necessari deve essere cancellata e i relativi supporti distrutti

Art. 5. Principio di Proporzionalità.

1. L'installazione di un sistema di controllo sarà proporzionato all'effettivo grado di rischio presente nell'area.
2. Il Titolare del trattamento valuterà in modo obiettivo se l'utilizzazione ipotizzata sia in concreto realmente proporzionata agli scopi prefissi e legittimamente perseguibili (art. 11, comma 1, lett. D) del Codice Privacy.
3. L' impianto di Videosorveglianza può essere attivato solo quando altre misure, come controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi e abilitazioni agli ingressi sono state ritenute insufficienti o inattuabili.
4. È vietata l'installazione di telecamere non funzionanti anche qualora non comporti trattamento di dati personali.

Art. 6. Principio di Finalità.

1. 1. Gli scopi perseguiti devono essere determinati, espliciti e legittimi (art. l i, comma 1, lett. B), del Codice Privacy.
2. 2. Il Titolare del trattamento dovrà comunicare nell'informativa le finalità perseguite dall'installazione di impianti di Videosorveglianza. L'informativa, basata sul modello predisposto dal Garante, deve essere chiaramente conoscibile e visibile da parte degli interessati.

TITOLO III —Soggetti.

Art. 7. Responsabili

Il Titolare del trattamento dei dati rilevati con il Sistema di Videosorveglianza è l'ISIS SERENI AFRAGOLA-CARDITO, rappresentato dal Dirigente Scolastico, dott.ssa Daniela Costanzo .

Il Titolare del trattamento ha il compito di vigilare sull'utilizzo del sistema di videosorveglianza e sul trattamento delle immagini in conformità agli scopi perseguiti e alle disposizioni di legge.

Il Titolare del trattamento può nominare uno o più Responsabili del trattamento dei dati (amministratore di sistema) quale funzionario responsabile delle operazioni relative al trattamento dei dati rilevati e conservati nel corso dell'attività di videosorveglianza e gli operatori (figura interna) che possono accedere con limitazioni di seguito indicate, alla postazione video.

Il Responsabile deve essere scelto tra i soggetti che per esperienza, capacità e affidabilità fornisca idonee garanzie del pieno rispetto delle disposizioni di legge in materia e del presente Regolamento.

I compiti affidati al Responsabile devono essere analiticamente specificati per iscritto dal Titolare del Trattamento dei dati. Il responsabile vigila sulla conservazione delle immagini e sulla loro distruzione al termine del periodo previsto per la conservazione delle stesse e assicura l'esercizio del diritto di accesso ai dati da parte dell'interessato o delle autorità competenti. Il Responsabile del trattamento deve designare per iscritto tutte le persone fisiche, incaricate del trattamento, in particolare stabilendo le modalità di accesso alle postazioni di controllo, a quelle di accesso alle modalità di conservazione dei supporti contenenti le immagini registrate, nonché quelle di utilizzo delle credenziali di accesso, individuando diversi livelli in corrispondenza delle specifiche mansioni attribuite ad ogni singolo incaricato. Il Responsabile del trattamento individua e nomina gli incaricati del trattamento dei dati personali tra i dipendenti dell'Istituto, in numero sufficiente a garantire la gestione del servizio di videosorveglianza. Il responsabile può altresì nominare quali incaricati del trattamento anche altri operatori o collaboratori esterni che, in ragione del proprio servizio e dell'attività svolta per l'Istituto, siano legittimati ad accedere ai dati del sistema di videosorveglianza (ad esempio gli addetti alla manutenzione dei sistemi). Gli incaricati, designati con apposito atto di nomina in cui sono definiti precisi compiti, devono trattare i dati personali ai quali hanno accesso attendendosi scrupolosamente alle istruzioni del responsabile, che vigila sulla loro corretta osservanza. Ad ogni incaricato vengono assegnate le credenziali ed uno specifico livello di accesso al sistema e sono istruiti al corretto uso del sistema, sulle disposizioni della normativa di riferimento e sul presente regolamento.

Il Dirigente Scolastico designa e nomina quale responsabile della gestione e del trattamento delle immagini il Sig. Russo G. a cui affida i compiti specifici sopra indicati con riferimento alle prescrizioni per l'utilizzo, gestione e manutenzione del sistema.

TITOLO V – Misure di sicurezza e gestione dei supporti.

Art. 14. Conservazione delle registrazioni.

Le immagini vengono custodite sull'hard disk per un tempo determinato in coerenza con quanto stabilito dal garante della privacy (48 ore) **a meno di ulteriori esigenze in relazione a festività**. Su specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria, la conservazione delle immagini e le modalità di ripresa potranno subire eccezioni al presente Regolamento.

I supporti di memorizzazione delle riprese contenenti dati sensibili devono essere opportunamente codificati senza ulteriori indicazioni di nominativi o di date.

I supporti non più utilizzati devono essere distrutti prima di essere cestinati.

Le immagini registrate non vengono archiviate e vengono messe a disposizione dell'Autorità Giudiziaria o di altre pubbliche Autorità in presenza di provvedimenti da queste emanati.

Art. 15. Centrale di Videosorveglianza — Accesso.

L'accesso alla Centrale in cui avviene la visualizzazione delle immagini (ove è posizionato il monitor) è consentito solamente al Responsabile del Trattamento, nonché agli incaricati, interni o esterni, per l'esercizio delle attività oggetto dell'incarico.

Operatori addetti alla manutenzione.

Possono essere autorizzati all'accesso soltanto i soggetti che devono provvedere a operazioni di manutenzione sugli impianti e nel locale ove questi sono collocati, nonché ufficiali e agenti di polizia giudiziaria nell'ambito delle loro specifiche attività di indagine. *Tali tecnici vengono nominativamente incaricati del trattamento e è fatto loro il divieto di asportare registrazioni o copie stampate delle immagini*. Gli addetti alle manutenzioni possono accedere alle immagini solo se ciò si rende indispensabile al fine di effettuare eventuali verifiche tecniche. L'accesso è consentito solo per scopi connessi alle finalità di cui al presente regolamento o per prestazioni strumentali agli stessi scopi. Gli incaricati e i preposti saranno dotati di credenziali personali di accesso al sistema. Le credenziali di accesso sono strettamente personali e non devono esser divulgate o cedute. I dati devono essere protetti da idonee misure di sicurezza conformi a quanto previsto dall'allegato B del Dlgs. N°196/2003. Le credenziali sono disattivate in caso di perdita della qualità che consente al responsabile, all'incaricato e al preposto l'accesso ai dati personali.

1. Le Centrali di Videosorveglianza sono posizionate in luoghi non facilmente accessibili e comunque controllati.
2. L'accesso/i sono sempre registrati.
3. I dispositivi di registrazione sono ulteriormente protetti da serratura.
4. I supporti di memorizzazione sono conservati in apposito armadio sotto chiave.

TITOLO VI – Diritti degli interessati (art. 7 D.Lgs. 196/03).

Art. 16. Diritti degli interessati.

1. Ai sensi dell'art. 7 del Codice Privacy, all'interessato è assicurato l'esercizio dei propri diritti, in particolare: a) accedere ai dati che li riguardano; b) verificare le finalità, le modalità e la logica del trattamento; c) ottenere l'interruzione di un trattamento illecito.
2. l'ISIS SERENI AFRAGOLA-CARDITO garantisce l'effettivo esercizio dei diritti dell'interessato, secondo le seguenti modalità: a) l'interessato, previa verifica dell'identità ed entro le ventiquattro ore successive alla rilevazione, può richiedere per iscritto l'accesso alle registrazioni che lo riguardano.

L'eventuale accesso a registrazioni riferite direttamente o indirettamente a terzi sarà oggetto di apposito bilanciamento degli interessi da parte del Responsabile della Unità Operativa; b) la visione e l'estrazione delle rilevazioni è gratuita per l'interessato, qualora sia portatore di interessi. Laddove ne ricorrano le condizioni, previa richiesta motivata dall'interessato, e relativa valutazione dei motivi, da parte del titolare del trattamento dei dati, la richiesta può essere accolta.

TITOLO VII – Prescrizioni e divieti.

Art. 17. Prescrizioni.

1. Il trattamento dei dati tramite sistemi di Videosorveglianza, le installazioni, le modalità organizzative e di gestione degli impianti seguiranno le norme del presente Regolamento.

Art. 18. Divieti.

1. Le operazioni non conformi al presente Regolamento, il trattamento illecito oppure non corretto dei dati, esporranno il Responsabile o l'Incaricato alle sanzioni amministrative, civili e penali previste dal Codice Privacy, nonché al regolamento emanato dal MINISTERO DELLA PUBBLICA ISTRUZIONE con decreto n. 305 del 7 dicembre 2006.

Art. 19. Nuove installazioni.

1. Ogni nuovo impianto dovrà seguire quanto previsto dal presente Regolamento.

La Dirigente Scolastica
Dott.ssa Daniela Costanzo