

Istituto Povere Figlie delle Sacre Stimmate

Scuola dell'Infanzia Baldini

Via dell'Oriolo 3 - 50041 - Calenzano (FI)

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO DATI

(Versione del 02/10/2023)

**Istituto Povere Figlie delle Sacre
Stimmate**

C.F. 02640920589

PEC:

*istitutopoverefigliedellesacrestimmate
@legalmail.it*

*Sede Legale
Via del Forte Trionfale 26,
00135 - Roma*

*Sede Operativa
Via dell'Oriolo 3,
50041 - Calenzano (FI)*

SEZIONE 1 - INTRODUZIONE

Sezione 1 . 1 Premessa

Il presente Documento rappresenta il Registro delle attività di trattamento dati della Scuola dell'Infanzia Baldini - Istituto Povere Figlie delle Sacre Stimmate, redatto nel rispetto della vigente normativa in materia di tutela della Privacy, ovvero ai sensi dell'art. 30 Regolamento UE n. 679/2016.

Sezione 1 . 2 Introduzione

Il presente Registro è redatto al fine di analizzare tutte le situazioni di trattamento di dati personali di cui la Scuola dell'Infanzia Baldini, nella persona della Legale Rappresentante Lobato Perez Maria Encarnacion, con sede legale in Roma, Via del Forte Trionfale 26, 00135 è titolare e per poter adottare le misure di sicurezza necessarie alla tutela dei dati trattati dallo stesso.

L'Istituto tratta, per gli adempimenti connessi all'attività educativa esercitata, una molteplicità di dati, tra i quali dati definiti dalla normativa "sensibili".

Il presente documento darà conto di tutte le misure adottate in relazioni alla tipologia delle varie banche dati.

I livelli di sicurezza indicati nel presente documento si applicano a tutti gli archivi di dati personali di competenza del Titolare.

Per ogni forma di trattamento (*elettronico, cartaceo, ecc..*) di dati originali o di copie sono definite modalità specifiche;

Le regole definite nel presente documento sono volte a prevenire violazioni della normativa sulla privacy ed a ridurre al minimo i rischi di accesso non autorizzato, di trattamento non conforme alle finalità, di distruzione o perdita dei dati.

Il personale, a qualunque titolo assunto, dall'Istituto deve essere informato sulle disposizioni contenute nel presente documento ed è tenuto ad applicarle per quanto di propria competenza.

Sezione 1 . 3 Glossario

Ai fini del presente documento si intende 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;
- **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;
- **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, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- **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;

- **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;
- **responsabile del trattamento**, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **incaricati**, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare;
- **interessato**, la persona fisica cui si riferiscono i dati personali;
- **consenso dell'interessato**, qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **violazione dei dati personali**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **Garante**, l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675 che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

SEZIONE 2 - TRATTAMENTI CON L'AUSILIO DI STRUMENTI ELETTRONICI

Sezione 2.1 Sistema di autenticazione Informatica

Tutti i trattamenti di dati personali in formato elettronico di cui l'Istituto è titolare sono accessibili soltanto attraverso una procedura di autenticazione. Per poter accedere al trattamento dei dati gli incaricati devono essere in possesso di credenziali individuali di autenticazione.

Come credenziali individuali l'Istituto si serve di password. In futuro potrà essere utilizzato qualunque altro strumento (badge, smartcard, ecc.) ritenuto idoneo all'identificazione nel rispetto della normativa sulla privacy.

Le credenziali di identificazione sono individuali e non possono essere rilasciate a più incaricati anche in tempi diversi. Ad ogni incaricato possono essere assegnate più credenziali per accessi differenziati a diverse banche di dati o a software gestionali.

All'atto del rilascio il personale è istruito sulle cautele e precauzioni da adottare per mantenere la sicurezza e affidabilità delle credenziali.

Le credenziali non utilizzate da almeno sei mesi devono essere disattivate; sono, altresì, tempestivamente disattivate al venire meno delle condizioni per cui erano state rilasciate e comunque al verificarsi di qualunque evento che ne possa compromettere la segretezza e l'efficacia.

La parola chiave è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

Gli incaricati sono tenuti a conservare e custodire con cura le credenziali e i dispositivi di autenticazione; è vietato comunicare le proprie credenziali a terzi.

In caso di allontanamento prolungato dal posto di lavoro gli incaricati avranno cura di chiudere tutte le applicazioni aperte che possono accedere ai dati personali.

Sezione 2.2 Misure di sicurezza

Si è provveduto:

- Ad installare e mantenere aggiornati dispositivi anti-intrusione per proteggere le reti informatiche da intrusioni dall'esterno con particolare attenzione alle reti collegate ad internet.
- A garantire che su tutti gli elaboratori siano presenti adeguati programmi di protezione da virus informatici e da tentativi di intrusione .
- Ad assicurarsi che su tutti i sistemi operativi installati negli elaboratori vengano installati gli aggiornamenti relativi alla sicurezza.
- Ad assicurarsi che tutte le disposizioni relative alle copie di sicurezza vengano osservate.

È espressamente vietato a tutti gli incaricati dei trattamenti:

- consegnare sotto qualunque forma a personale non autorizzato elaborati o copie dei dati oggetto del trattamento;
- comunicare a personale non autorizzato notizie relative a dati personali o sensibili trattati;
- effettuare copie non autorizzate dei dati oggetto del trattamento;

Sezione 2.3 Registro delle attività di trattamento dati

Sarà cura del Titolare mantenere aggiornato il presente documento al variare delle situazioni relative ai trattamenti di dati effettuati dall'Istituto. Per ogni trattamento è indicata la categoria dei dati (se ordinari, o sensibili o giudiziari) in relazione alle informazioni contenute negli archivi.

Sezione 2.4 Misure da adottare per garantire l'integrità e la disponibilità dei dati

Tutti i trattamenti sono effettuati nei locali dell'Istituto, ove opera personale dipendente.

Le misure di sicurezza adottate e da adottare sono quelle riportate nella tabella 1 per quanto riguarda i dati trattati con l'utilizzo di strumenti elettronici, e quelle riportate nella tabella 2 per i dati trattati senza l'ausilio di strumenti elettronici.

Ulteriori misure adottate:

- I locali in cui avvengono i trattamenti di dati non sono accessibili al pubblico se non in maniera programmata (esempio: colloqui o appuntamenti per incontri /riunioni);
- In caso di allontanamento prolungato dal posto di lavoro gli incaricati avranno cura di chiudere tutte le applicazioni aperte che possano dare accesso a dati personali.
- Durante le operazioni di pulizia dei locali il sistema informatico è disattivato e comunque le procedure informatiche non sono accessibili.
- I locali sono provvisti di chiave.

Sezione 2.5 Criteri e modalità di ripristino della disponibilità dei dati

Le misure adottate dal Titolare devono garantire il ripristino di qualunque banca dati oggetto di trattamento entro 72 ore.

Durante il ripristino delle copie e in presenza di dati sensibili devono essere adottate le stesse misure di sicurezza che si applicano ai trattamenti;

Gli interventi di ripristino di archivi che contengono dati sensibili effettuati da personale esterno devono essere effettuati in presenza di personale autorizzato dell'Istituto.

SEZIONE 3 - TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Sezione 3.1 Individuazione trattamenti

La documentazione è conservata in luoghi non accessibili a personale non autorizzato e, in presenza di dati sensibili in armadi muniti di chiave.

Tutti i dati sono raccolti per perseguire finalità istituzionali o in ottemperanza a disposizioni normative e regolamentari. La documentazione relativa allo stato di salute è classificata come dato sensibile (certificati medici ecc.) è conservata all'interno del fascicolo personale in una apposita sezione separata dalla corrispondenza comune. Tutti i trattamenti vengono conservati agli atti per il periodo obbligatorio per legge.

Ulteriori misure adottate:

- Durante le operazioni di pulizia dei locali la documentazione con dati personali risulta non accessibile;
- I locali e gli armadi contenenti documentazione sono provvisti di chiave.

Le misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati il cui trattamento è effettuato su supporti cartacei sono quelle individuate nella tabella 2.

Sezione 3.2 Incaricati

Agli incaricati al momento della nomina deve essere consegnata apposita lettera di incarico contenente copia delle "norme comportamentali per gli incaricati del trattamento di dati personali" adottate dal Titolare. Nell'ambito delle indicazioni contenute nel loro mandato gli Incaricati sono in particolare tenuti a:

- Informare tempestivamente il Titolare di qualunque evento che pregiudichi la sicurezza dei dati;
- Custodire le pratiche e i documenti loro affidati e restituirli al termine del trattamento avendo cura che agli stessi non avvengano accessi non autorizzati;
- Osservare le misure di sicurezza ai sensi delle normative e dei disciplinari tecnici vigenti in materia di dati personali;
- Osservare le disposizioni impartite dal Titolare anche tramite il presente documento;

È espressamente vietato a tutti gli incaricati dei trattamenti:

- consegnare sotto qualunque forma a personale non autorizzato copie dei dati oggetto del trattamento;
- comunicare a personale non autorizzato notizie relative a dati personali o sensibili trattati;
- effettuare copie non autorizzate dei dati oggetto del trattamento;

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DATI

TITOLARE: Istituto Povere Figlie delle Sacre Stimmate - Legale Rappresentante: Lobato Perez Maria Encarnacion

Indirizzo Pec: istitutopoverefigliedellesacrestimmate@legalmail.it

DPO: DOTT. JACOPO FERRARO - Indirizzo Pec: jacopoferraro@legalmail.it

Tipologia di Trattamento	Finalità e Basi legali del Trattamento	Categorie di Interessati	Categorie di Dati Personali	Categorie di Destinatari	Trasferimento Dati verso Paesi Terzi o Organizzazioni Internazionali	Termini Ultimi di Cancellazione Previsti	Misure di Sicurezza Tecniche e Organizzative
Gestione Giuridica del Personale	Attività di gestione e amministrazione del personale, con riferimento a: 1. Adempimento degli obblighi relativi al contratto di lavoro e/o leggi o norme cogenti; 2. Adempimento disposizioni inerenti gli istituti previdenziali e assistenziali, anche integrativi, e relativi a quelli assicurativi.	Personale Dipendente	Dati personali e dati sensibili	Enti Previdenziali: Inps, Inail Studio di Consulenza del Lavoro titolare autonomo del trattamento	No	I documenti vengono conservati per un tempo non inferiore a 10 anni dalla cessazione del rapporto di lavoro/collaborazione, comunque nel rispetto dei termini definiti dalla normativa applicabile.	Vedere Scheda Apposita
Gestione Economica del Personale	Attività di gestione e amministrazione del personale, con riferimento a: 1. Redazione buste paghe in riferimento al CCNL e alle leggi/norme cogenti; 2. Amministrazione del rapporto di lavoro	Personale Dipendente	Dati personali e dati sensibili	Enti Previdenziali: Inps, Inail Studio di Consulenza del Lavoro titolare autonomo del trattamento	No	I documenti vengono conservati per un tempo non inferiore a 10 anni dalla cessazione del rapporto di lavoro/collaborazione, comunque nel rispetto dei termini definiti dalla	Vedere Scheda Apposita

	(gestione permessi, ferie, malattie, ecc.)					normativa applicabile.	
Acquisizione CV	Ricerca del Personale	Candidati che rilasciano CV	Dati personali e dati sensibili		No	I documenti relativi ai candidati vengono conservati per un tempo non superiore ai 12 mesi dell'ultimo contatto.	Vedere Scheda Apposita
Gestione acquisti di beni e servizi e relativi contratti	Acquisizione beni e servizi necessari per il funzionamento dell'Istituto	Imprese Individuali o società che forniscono beni e servizi limitatamente ai dati di loro soci o amministratori	Dati ordinari e dati contabili	Studio Commercialista Titolare autonomo del trattamento	No	I documenti vengono conservati per un tempo non inferiore a 10 anni dalla cessazione del rapporto di lavoro/collaborazione, comunque nel rispetto dei termini definiti dalla normativa applicabile.	Vedere Scheda Apposita
Gestione amministrativa iscrizioni alunni	Esecuzione del contratto avente oggetto l'attività didattica	Alunni, familiari degli alunni	Dati ordinari e dati contabili, dati personali e dati sensibili	Studio Commercialista Titolare autonomo del trattamento Comune di Calenzano Miur	No	I documenti vengono conservati per un tempo non inferiore a 10 anni dall'uscita del bambino dall'Istituto.	Vedere Scheda Apposita
Gestione dell'attività scolastica	Nell'espletamento delle attività propedeutiche all'avvio dell'anno scolastico da parte	Alunni	Dati personali e dati sensibili	\\	No	I documenti vengono conservati per un tempo non inferiore a 10 anni dall'uscita del bambino dall'Istituto.	Vedere Scheda Apposita

	dell'Istituto, possono essere trattati dati sensibili come ad esempio dati relativi alle origini razziali ed etniche, per favorire l'inserimento degli alunni con cittadinanza non italiana; allo stato di salute, per assicurare sostegno agli alunni diversamente abili e per la composizione delle classi.						
Raccolta materiale fotografico	L'istituto, previo consenso dei genitori, raccoglie materiale fotografico inerente alle attività didattiche svolte dagli alunni. Le foto possono essere utilizzate per mostre scolastiche riservate ai genitori degli alunni o per eventi promozionali organizzati dalla Scuola. La Responsabile, all'interno dell'istituto, fa operazioni di raccolta, cancellazione e di montaggio del materiale fotografico.	Alunni	Dati personali	\\	No	I documenti vengono conservati per un tempo non inferiore a 10 anni dall'uscita del bambino dall'Istituto.	Vedere Scheda Apposita

Incarichi professionali e relativi contratti	Conferire incarichi necessari per la gestione o tutela Del'Istituto	Liberi professionisti che collaborano con il Titolare	Dati ordinari	Studio Commercialista Titolare autonomo del trattamento	No	I documenti vengono conservati per un tempo non inferiore a 10 anni dalla cessazione del rapporto di lavoro/collaborazione, comunque nel rispetto dei termini definiti dalla normativa applicabile.	Vedere Scheda Apposita
Sorveglianza sanitaria e attività di formazione obbligatoria in base al D.Lgs. n. 81/2008	Attività obbligatoria in base alla normativa sulla sicurezza D.Lgs. n. 81 del 2008	- Dipendenti - Collaboratori	Dati Particolari (Dati Sensibili)	- Medico Competente - Organi Pubblici di vigilanza in caso di ispezioni	No	I documenti vengono conservati per un tempo non inferiore a 10 anni dalla cessazione del rapporto di lavoro/collaborazione, comunque nel rispetto dei termini definiti dalla normativa applicabile.	Vedere Scheda Apposita

Tabella 1 – MISURE DI SICUREZZA ADOTTATE E DA ADOTTARE PER DATI TRATTATI CON STRUMENTI ELETTRONICI

Misure	Descrizione dei rischi	Trattamenti in essere	Misure in essere	Misure da adottare e tempi previsti per l'adozione
Istruzioni agli incaricati	Eventi relativi ai comportamenti degli operatori: - furto delle credenziali di autenticazione; - carenza di consapevolezza, disattenzione o incuria; - comportamenti sleali o fraudolenti; - azione di virus informatici o altre tecniche di sabotaggio intercettazione di informazioni in rete; - errore materiale	Tutti i trattamenti informatizzati	Si	(ad ogni nuova assunzione o incarico o variazione di mansione)
Formazione		Tutti i trattamenti informatizzati	Si	(ad ogni nuova assunzione o incarico o variazione di mansione)
Presenza di: - antivirus		Tutti i trattamenti informatizzati	Si	//
Controllo dell'accesso ai locali che sono chiusi a chiave quando non presidiati, divieto di accesso ai locali alle persone non autorizzate		Tutti i trattamenti informatizzati	Si	//
Profilo di autorizzazione che non consenta la formattazione dei dischi fissi		Tutti i trattamenti informatizzati	Si Non ci sono utenti con profilo di amministratore che possono creare tali inconvenienti	//
Presenza di: - antivirus	eventi relativi agli strumenti: - azione di virus informatici o di codici malefici; - malfunzionamento, indisponibilità o degrado degli strumenti; - accessi esterni telematici non autorizzati; - intercettazione di informazioni	Tutti i trattamenti informatizzati	Si	//
Istruzioni agli incaricati atte a individuare e prevenire le situazioni a rischio		Tutti i trattamenti informatizzati	Si	(ad ogni nuova assunzione o incarico o variazione di mansione)

	in rete			
Chiusura a chiave dei locali quando non presidiati: istruzioni a tutti gli operatori	Eventi relativi al contesto: - accessi non autorizzati ai locali; - asportazione e furto di strumenti contenenti dati; - eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria; - guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc...); - errori umani nella gestione della sicurezza fisica	Tutti i trattamenti informatizzati	Si	(ad ogni nuova assunzione o incarico o variazione di mansione)
Disponibilità di estintori come da normativa antincendio		Tutti i trattamenti informatizzati	Si	//
Il backup avviene su apposito hard disk esterno conservato in una stanza dedicata, chiusa a chiave		Tutti i trattamenti informatizzati	Si	//
Verifica della congruità dei locali rispetto a rischi di infiltrazioni d'acqua, incendio, inondazioni, terremoti		Tutti i trattamenti informatizzati	Si	//
Verifica della logistica degli apparecchi e del loro corretto posizionamento		Tutti i trattamenti informatizzati	Si	//

TABELLA 2 - MISURE DI SICUREZZA ADOTTATE E DA ADOTTARE PER DATI TRATTATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Misure	Descrizione dei rischi	Trattamenti in essere	Misure in essere	Misure da adottare e tempi previsti per l'adozione
Istruzioni agli incaricati	Eventi relativi ai comportamenti degli operatori: - carenza di consapevolezza, disattenzione o incuria; - comportamenti sleali o fraudolenti; - accessi esterni non autorizzati;	Tutti i trattamenti cartacei	Si	//
Custodia dei documenti in armadi chiusi a chiave		Tutti i trattamenti cartacei	Si	//
Controllo dell'accesso ai locali che sono chiusi a chiave quando non presidiati, divieto di accesso ai locali alle persone non autorizzate		Tutti i trattamenti cartacei	Si	//

	- errore materiale			
Chiusura a chiave dei locali quando non presidiati: istruzioni a tutti gli operatori	eventi relativi al contesto: - accessi non autorizzati ai locali; - asportazione e furto di fascicoli (o altri contenitori) contenenti dati; - eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria; - guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc...); - errori umani nella gestione	Tutti i trattamenti cartacei	Si	//
Disponibilità di estintori come da normativa anti-incendio		Tutti i trattamenti cartacei	Si	//
Disponibilità di armadi muniti di chiusura a chiave		Tutti i trattamenti cartacei	Si	Verifica periodica del buon funzionamento di serrature degli armadi
Verifica della congruità dei locali rispetto a rischi di infiltrazioni d'acqua, incendio, inondazioni, terremoti		Tutti i trattamenti cartacei		//

Calenzano, 02 Ottobre 2023