ISTITUTO COMPRENSIVO STATALE "N. IANNACCONE"

Via Ronca, 11, 83047, LIONI, AV

Tel. 082742046, Email: avic86000t@istruzione.it

ISTITUTO COMPRENSIVO STATALE - "N. IANNACCONE"-LIONI
Prot. 0002813 del 25/05/2018
01-01 (Uscita)

MANUALE DELLA PRIVACY

Emesso da: Commissione Privacy d'Istituto
Verificato da: Il Responsabile del trattamento
Approvato da: Il Dirigente Scolastico

Il Dirigente scolastico Dott.ssa Cristina NOVI	Il Responsabile del trattamento Paolo Garofalo

1. SCOPO DEL MANUALE

Al fine di gestire correttamente gli adempimenti connessi al Regolamento UE 2016/679 (regolamento generale sulla protezione dei dati), nonché per creare e sostenere la cultura della privacy all'interno dell'istituzione scolastica,è stato elaborato il presente "Manuale della Privacy" da tenere periodicamente aggiornato sia in base all'evoluzione della normativa in materia di trattamento e protezione dei dati personali sia in occasione di rilievi conseguenti a novità delle modalità del trattamento dei dati.
Il presente manuale è anche uno strumento operativo per la tutela della riservatezza dei dati personali in rapporto all'assetto organizzativo dell'istituzione scolastica. Compito del presente documento è infatti quello di individuare, descrivere e definire:

- le responsabilità, nonché le istruzioni impartite ai soggetti preposti al Trattamento;
- le linee generali delle azioni necessarie per il monitoraggio del processo del trattamento dei dati personali in base ad una preventiva e dettagliata analisi dei rischi volta all'individuazione ed alla consequenziale adozione delle misure di sicurezza;
- gli adempimenti necessari, sia a rilevanza interna che esterna;
- le procedure per la tutela della riservatezza dei dati personali in rapporto all’assetto organizzativo dell'istituto scolastico.

2. GESTIONE DEL MANUALE E DELLA DOCUMENTAZIONE DI SUPPORTO

2.1.Gestione del manuale

Le responsabilità riguardo all’emissione, alla verifica e all'approvazione del presente manuale sono così suddivise:

Attività	Responsabilità
Emissione	Commissione Privacy
Verifica	Responsabile del Trattamento
Approvazione	Dirigente Scolastico

Il presente manuale è tenuto ed aggiornato dal Responsabile del Trattamento e dalla Commissione Privacy.

Tali soggetti hanno l’obbligo di curare:

- la revisione periodica, formulando le proposte di modificazione e integrazione al Titolare del Trattamento;
- la corretta applicazione e conservazione del manuale;
- la distribuzione del medesimo, anche per via telematica.

Sul frontespizio del manuale è riportato l'indice di revisione e la data di emissione dello stesso.

2.2.Documentazione di supporto

Costituiscono documentazione di supporto alla gestione del sistema di protezione dati adottato dall'istituto, gli allegati riportati in tabella.

Allegato	Contenuti
Analisi dei rischi	In questo allegato sono riportati gli eventi considerati potenzialmente dannosi per la sicurezza dei dati e i risultati della valutazione del livello di rischio ad essi associato (in relazione alla gravità di danno e alla probabilità di accadimento).

Disciplinare interno sull'uso della posta elettronica e di internet	L'allegato descrive le caratteristiche e le regole di utilizzo della rete Internet e della posta elettronica da parte del personale e, contestualmente, ha l'obiettivo di informare i lavoratori sui controlli effettuati e sul trattamento eseguito sui loro dati personali.
Elenco hardware	In questo allegato sono riportati, in forma sintetica, gli elaboratori utilizzati per i trattamenti svolti con l'ausilio di strumenti elettronici, eventuali base dati in essi contenuti e le misure di sicurezza informatica adottate.
Elenco misure adottate	In questo allegato sono riportate, in forma sintetica, le misure in essere a protezione dei dati personali trattati.
Elenco software	In questo allegato sono riportati, in forma sintetica, i software autorizzati
Mansionario	L'allegato individua la distribuzione dei compiti e delle responsabilità all'interno dell'organizzazione.
Piano di formazione	In questo allegato sono riportate le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.
Piano di miglioramento	In questo allegato sono riportate le misure da adottare per contrastare i rischi individuati. Per ciascun intervento vengono riportati il termine temporale entro il quale procedere al completamento dell'azione e il responsabile della sua esecuzione.
Registro audit	In questo allegato vengono riportate le informazioni relative agli audit svolti e/o pianificati.
Registro delle attività di trattamento	Il registro contiene le informazioni relative ai trattamenti svolti dal titolare e/o per conto del titolare da parte di fornitori esterni, secondo quanto disposto dall'art. 30 del Regolamento UE 2016/679.
Registro eventi	In questo allegato vengono riportate le informazioni relative ad eventi (potenziali e non) che hanno (o avrebbero potuto) recare danno ai dati personali trattati presso l'istituto. Le segnalazioni raccolte mediante i moduli "Scheda di segnalazione" - disponibili presso gli uffici di segreteria - costituiscono un valido strumento di monitoraggio del sistema di protezione dei dati personali adottato dall'istituto, consentendo agevolmente di rilevare eventuali criticità dello stesso, e allo stesso tempo rappresentano un'efficace metodo di coinvolgimento del personale.
Scheda backup	L'allegato riporta i criteri adottati per il salvataggio dei dati e la gestione delle copie di sicurezza delle base dati.

La finalità di questi documenti è quella di dare evidenza oggettiva delle attività eseguite e dei controlli previsti all'interno delle procedure del sistema privacy.
Gli allegati vengono aggiornati periodicamente, con cadenza almeno annuale in occasione della revisione periodica del sistema di gestione privacy adottato dall'istituto. Lo stato di revisione è riportato su ciascun allegato.
Il Registro delle attività di trattamento viene aggiornato ad ogni modifica delle informazioni in esso contenute.

3. RIFERIMENTI NORMATIVI

Norma	Descrizione
Decreto legislativo n. 196/03	Testo Unico in materia di protezione dei dati personali
Allegato B – D.Lgs. n. 196/03	Disciplinare tecnico per l'individuazione e l'applicazione delle misure minime di sicurezza per il Trattamento dei dati personali
Decreto n. 305 del 7 dicembre 2006	Regolamento relativo al trattamento dei dati sensibili e giudiziari nel settore dell'istruzione
Del. del Garante n.13 del 1 Marzo 2007	Linee guida del Garante per posta elettronica e internet
Provvedimento del Garante del 27/11/2008	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema
Regolamento UE 2016/679	Regolamento generale sulla protezione dei dati

4. DEFINIZIONI PRINCIPALI

Per una corretta, puntuale ed analitica applicazione delle norme di cui al citato Testo Unico in materia di protezione dei dati personali, si riportano di seguito le principali definizioni:

Definizioni generali

"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;

"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;

"dati identificativi": i dati personali che permettono l'identificazione diretta dell'interessato;

"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;

"dati genetici": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

"dati biometrici": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche

fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

"dati relativi alla salute": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

"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

"titolare": la persona fisica o 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;

"responsabile": 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 o dal responsabile;

"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;

"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;

"diffusione": il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

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

"pseudonomizzazione": 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;

"blocco": la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

"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;

"Garante": l'autorità di controllo di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675;

"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;

"chiamata": la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

"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;

"rete pubblica di comunicazioni": una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

"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;

"posta elettronica": messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Definizioni riguardanti le misure di sicurezza

"misure di sicurezza", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello di protezione richiesto in relazione ai rischi presenti;

"strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

"autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

"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;

"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;

"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;

"sistema di autorizzazione", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

5. RUOLI E RESPONSABILITA'

Il seguente funzionigramma fornisce una descrizione sintetica della struttura dell'organizzazione scolastica e degli ambiti di competenza attribuite alle figure ed unità operative preposte al trattamento dei dati.

Struttura	Responsabile	Compiti

Amministratori di sistema	Dirigente Scolastico	Gestione e manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle base dati, le reti locali e gli apparati di sicurezza, nella misura in cui consentono di intervenire sui dati personali.
Backup operator	Responsabile del trattamento interno	Esecuzione delle copie di backup e delle prove di ripristino dei database.
Collaboratori del Dirigente Scolastico	Dirigente Scolastico	Affiancamento al D.S. con deleghe parziali e sostituzione dello stesso in caso di assenza.
Collaboratori scolastici	D.S.G.A.	Apertura e chiusura della sede, custodia e controllo, consegna e ricezione plichi e lettere, pulizia, assistenza a tutte le altre attività, gestione di dati comuni di alunni, docenti e familiari.
Commissione Privacy	Dirigente Scolastico	Assistenza alla direzione scolastica nella gestione delle questioni attinenti la privacy.E' composta da personale interno con comprovate conoscenze giuridiche e/o tecnologiche e si occupa di segnalare ai rapprensentanti della direzione o ai responsabili del trattamento, eventuali innovazioni di natura normativa o tecnologica che possono rendere inadeguato il sistema di gestione privacy dell'istituto e di proporre nuove misure e accorgimenti per la protezione dei dati.
Corpo Docente	Dirigente Scolastico	Insegnamento e attività integrative e collaterali, partecipazione alle scelte organizzative e di orientamento generale, partecipazione alla gestione di specifiche attività (Biblioteca, scelte degli acquisti, commissioni varie, ecc,)
Direttore dei servizi generali e amministrativi		Supervisione e della gestione amministrativo-contabile e coordinamento delle attività di segreteria e dei collaboratori scolastici
Dirigente Scolastico		Responsabilità della gestione del sistema di tutela e protezione dei dati trattati presso o per conto dell'istituto scolastico.
Preposti alla custodia delle password	Responsabile del trattamento interno	Conservazione e custodia delle copie di credenziali di accesso, utilizzate dagli operatori addetti al'utilizzo degli strumenti informatici.
Responsabili controllo accessi ai locali	Responsabile del trattamento interno	Controllo degli accessi e dei sistemi di accesso ai locali in cui si svolgono operazioni di trattamento di dati personali.
Responsabili del Trattamento	Dirigente Scolastico	Le funzioni attribuite concernano: l'organizzazione delle operazioni di trattamento dei dati; l'individuazione e aggiornamento degli incarichi e dei loro ambiti di trattamento;la vigilanza del rispetto delle istruzioni impartite agli incaricati del trattamento;la conservazione e custodia della documentazione concernente il sistema di gestione privacy; il monitoraggio delle misure di sicurezza adottate.
Segreteria amministrativa	D.S.G.A.	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente.

L'elenco aggiornato dei preposti addetti all'utilizzo di strumenti informatici e delle altre figure del sistema di gestione privacy (responsabili del trattamento, amministratori di sistema, responsabili controllo accessi, preposti alla custodia delle passwword) è riportato nell'allegato titolato "Mansionario".

L'individuazione delle suddette figure - con eccezione degli incaricati del trattamento - viene effetuata tra i soggetti che per esperienza, capacità ed affidabilità, sono in grado di fornire adeguate garanzie di rispetto delle disposizioni vigenti in materia di trattamento di dati personali.

La designazione di questi soggetti è individuale e nominativa. La nomina avviene per iscritto e il destinatario della designazione firma il documento per accettazione dell'incarico. Nella lettera di nomina vengono riportati in maniera analitica gli ambiti di operatività consentiti.

Le suddette nomine non esimono comunque il Titolare dall'obbligo di vigilare, anche tramite verifiche periodiche, sulla puntuale osservanza delle disposizioni in materia di Trattamento e delle istruzioni impartite.

E' opportuno precisare che la nomina del responsabile del trattamento è a discrezione del Dirigente scolastico, il quale - in ragione delle esigenze organizzative dell'istituto - può designare anche mediante suddivisione di compiti più responsabili del trattamento.
La nomina di responsabile del trattamento può riguardare anche soggetti esterni operanti in nome e per conto del Titolare: in tal caso il trasferimento di dati personali dall'Istituto al soggetto esterno non è qualificabile tecnicamente come una comunicazione di informazioni, per cui non necessita di acquisizione preventiva del consenso espresso dell'interessato.

Per quanto riguarda gli amministratori di sistema, invece, si rileva che le prescrizioni riguardanti i titolari dei trattamenti effettuati con strumenti elettronici, di cui al provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, non si applicano a quei soggetti che dotati di sistemi informatici di modesta e limitata entità e comunque non particolarmente complessi, possono fare a meno di figure professionali specificamente dedicati all'amministrazione di sistemi o comunque abbiano ritenuto di non farvi ricorso, e pertanto - considerata l'infrastruttura tecnologica dell'istituto - anche la designazione di eventuali amministratori di sistema è da considerarsi un atto discrezionale del dirigente scolastico.

In nessun caso possono essere nominati amministratori di sistemi, soggetti che solo occasionalmente intervengono (per esempio per scopi di manutenzione a seguito di guasti o malfunzionamenti) sui sistemi di elaborazione e sui sistemi software dell'istituto.

5.1. La Commissione Privacy

La Commissione Privacy non è un organo previsto dalla normativa vigente in materia di protezione dei dati personali. Tuttavia, considerati gli obblighi della normativa sulla Privacy e la necessità di procedere al meglio ad una serie di adempimenti, sia a rilevanza interna che esterna, l'Istituto Scolastico, in persona del suo Dirigente Scolastico, ha ritenuto opportuno delineare i tratti ed i requisiti al fine della sua costituzione.
La Commissione è costituta da:

- soggetti con qualificata formazione giuridica, che possiedono un'adeguata conoscenza della normativa sul trattamento dei dati personali e delle problematiche giuridiche ad essa sottese;
- personale con competenze gestionali, cui è demandata la revisione delle procedure gestionali degli adempimenti ed il monitoraggio dei flussi informativi interni all'Istituto e verso l'esterno;
- personale tecnico-informatico, in grado di apportare il proprio contributo soprattutto in relazione alla valutazione dei rischi e all'adozione delle misure di sicurezza.

Spetta al Dirigente Scolastico (o ad un suo delegato) presiedere, coordinare, controllare e convocare la commissione.

5.2. Nomina e formazione degli incaricati

Per l'esplicazione del corretto e legittimo trattamento dei dati personali di cui l'istituto scolastico è in possesso, il Dirigente scolastico ha provveduto a nominare il personale A.T.A. e il personale docente (in servizio presso codesta istituzione scolastica) "incaricati del trattamento" e ciò in quanto, in assenza di formale nomina e di adeguato piano di formazione, il medesimo personale non potrebbe accedere legittimamente ai dati personali, né compiere operazioni di trattamento in osservanza delle disposizioni del Regolamento UE 2016/679.

La designazione degli incaricati è individuale e nominativa. All'atto della nomina vengono consegnate all'incaricato le linee guida, recanti istruzioni operative relative all'ambito di trattamento consentito, in funzione del profilo professionale di appartenenza.
Sessioni formative vengono pianificate con cadenza almeno annuale, allo scopo di rendere edotto il personale addetto ai trattamenti sui possibili rischi relativi al trattamento delle informazioni e sulle minacce alla sicurezza delle informazioni.
La formazione è predisposta per tutti i dipendenti, sia in occasione di un nuovo ingresso in servizio, che di cambiamento di mansione o di introduzione di nuove tecnologie hardware e software.

È compito del responsabile del trattamento:

- rilevare il bisogno di interventi formativi;
- organizzare gli stessi compatibilmente con le esigenze dell'attività lavorativa;
- redigere il piano di formazione;
- raccogliere l'elenco dei partecipanti di ogni singolo corso e informarli dettagliatamente sullo stesso (contenuti, obiettivi, modalità di svolgimento, ecc.);
- vigilare sul rispetto del programma dell'attività formativa;
- vigilare sulla partecipazione dei corsisti.

6. ADEMPIMENTI A RILEVANZA INTERNA

Gli adempimenti definiti a rilevanza interna riguardano:

1. l'adozione di misure di sicurezza;
2. la distribuzione dei compiti di effettuazione delle copie di backup delle banche dati gestite con strumenti informatici;
3. il controllo del processo di trattamento.

6.1. Adozione delle misure di sicurezza

Il Testo Unico in materia di trattamento di dati personali prevede l'obbligo di adozione di idonee misure di sicurezza, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del Trattamento, in modo da ridurre al minimo i rischi di:

1. distruzione o perdita, anche accidentale, dei dati stessi;
2. accesso non autorizzato;
3. trattamento non consentito o non conforme alle finalità della raccolta.

In adempimento di quanto sopraesposto, l'Istituto Scolastico ha provveduto ad adottare una serie di azioni, secondo uno schema logico e una serie di tecniche derivate dal risk-management, che si sono concretizzate in una dettagliata individuazione e valutazione dei rischi connessi al Trattamento dei dati personali.

Le fasi, che caratterizzano questo processo, sono:

<u>1. Ricognizione dei trattamenti e delle misure adottate</u>

Essa ha l'obiettivo di evidenziare il numero e la tipologia di trattamenti, i locali adibiti al trattamento dei dati, le risorse hardware e software utilizzate nelle operazioni di trattamento, le misure di sicurezza adottate. Gli output di questa fase sono costituiti dagli allegati:
"Registro delle attività di trattamento",
"Elenco hardware",
"Elenco misure adottate",
"Elenco software"

2. Analisi e valutazione dei rischi

Il monitoraggio dei rischi che incombono sui dati trattati con strumenti informatici e non, sulle aree e i locali in cui avvengono le operazioni di trattamento, e sulle modalità di trattamento, con particolare attenzione per i collegamenti in rete, viene effettuato mediante l'uso di apposite check list, contenute all'interno della piattaforma Argo Privacy WEB. Una volta evidenziati i rischi presenti, si provvede ad assegnare ad ogni fattore di rischio un indice numerico relativo alla probabilità di accadimento di un evento dannoso (P) e alla "gravità" del danno che potrebbe conseguirne (D). La stima del livello di rischio è espressa come prodotto dei due indici: R = PxD

La probabilità e la magnitudo, misurate in scala 1-4, danno origine alla seguente matrice di rischio

	MAGNITUDO			
PROBABILITÀ	**1 (nessun danno)**	**2 (danni lievi)**	**3 (danni medi)**	**4 (danni gravi)**
4 (alta)	4	8	12	16
3 (media)	3	6	9	12
2 (bassa)	2	4	6	8
1 (nulla)	1	2	3	4

Il rischio è valutato sulla base della seguente legenda

	rischio accettabile
	rischio basso
	rischio medio
	rischio elevato

L'output del processo di analisi e di valutazione dei rischi è costituito dall'allegato titolato "Analisi dei rischi".

3. Monitoraggio e Miglioramento

Sulla base delle risultanze emerse dall'analisi dei rischi, il titolare del trattamento, provvede, a seguito consultazione con i responsabili interni del trattamento, il responsabile della protezione dati, ed eventuali altre figure facenti parte della commissione privacy, a pianificare eventuali interventi formativi o di aggiornamento per gli incaricati del trattamento e l'implementazione di ulteriori misure di sicurezza volte a ridurre i rischi residui.
Il sistema di protezione dati adottato dall'organizzazione è monitorato attraverso due strumenti:
- audit interni, per la verifica della conformità dell'organizzazione e della struttura ai requisiti del sistema
- schede di segnalazioni di violazioni dei dati personali

Gli output di questa fase sono costituiti dagli allegati:

"Piano di formazione",
"Piano di miglioramento" (riportante l'elenco delle misure che si intende implementare)
"Registro Audit" (riportante l'elenco degli audit svolti e pianificati)
"Registro Eventi" (riportante l'elenco delle segnalazioni relative a rischi nella gestione dei dati personali o

episodi di violazione dei dati)

6.2. Distribuzione dei compiti di effettuazione delle copie di backup delle banche dati.
Per rispondere in maniera efficiente a situazioni di emergenza quali la distruzione o il danneggiamento dei dati o degli strumenti elettronici con cui avviene il trattamento degli stessi, si è provveduto ad individuare, tra i preposti all'utilizzo di strumenti informatici, gli incaricati delle copie di sicurezza delle banche dati (backup operator). È onere del Responsabile del trattamento individuare, in relazione all'attività svolta dagli operatori, uno o più incaricati delle copie di sicurezza, e stabilire (eventualmente con il supporto del responsabile tecnico dell'istituto), in relazione al tipo di rischio potenziale e in base alla tecnologia utilizzata, la periodicità con cui effettuare le copie di sicurezza, il tipo di supporto da utilizzare per le copie di backup, la periodicità con cui effettuare le prove di ripristino e la durata massima di conservazione delle copie (v. allegato "Scheda backup).
E' compito degli Incaricati delle copie di sicurezza delle banche dati assicurarsi della qualità delle copie di sicurezza dei dati e segnalare tempestivamente al Responsabile del trattamento ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

6.3. Il controllo del processo di trattamento
È obbligo degli incaricati del trattamento provvedere a che i dati raccolti siano:

- trattati in modo lecito e secondo correttezza;
- esatti, e se necessario aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

In particolare, nel caso di trattamento di dati sensibili e giudiziari, l'incaricato dovrà procedere nel rispetto delle prescrizioni contenute nel D.M. n. 305/2006 e nelle schede ad esso allegate.

In caso di cessazione di un trattamento, gli incaricati dovranno attenersi alle disposizioni del Dirigente scolastico o del Responsabile del trattamento.

Il controllo sul processo di trattamento dei dati, svolto attraverso verifiche ispettive interne, è a cura del Responsabile della protezione dati, eventualmente coaudivato dalla Commissione Privacy. L'azione di monitoraggio dovrà altresì accertare:

- le finalità del Trattamento, ossia gli scopi per cui i dati vengono raccolti e successivamente trattati ;
- le modalità di Trattamento, ossia gli strumenti che vengono utilizzati per trattare i dati;
- la natura dei dati trattati (es. comuni, sensibili o giudiziari);
- l'ambito di comunicazione e diffusione;
- i profili di autorizzazione dei preposti al trattamento con strumenti informatici.

7. ADEMPIMENTI A RILEVANZA ESTERNA

Gli adempimenti definiti a rilevanza esterna riguardano:

1. le modalità utilizzate per la predisposizione delle informative agli interessati;
2. le modalità per favorire l'esercizio dei diritti da parte dell'interessato.

7.1. Informative all'Interessato
Gli artt. 13 e 14 del Regolamento UE 2016/679 indicano una serie di elementi che devono essere necessariamente presenti nell'informativa che l'Istituto Scolastico, nella qualità di Titolare del Trattamento dei dati personali, deve obbligatoriamente rendere all'interessato o alla persona presso la quale sono raccolti i

dati.

Le informazioni da fornire riguardano, tra l'altro:

1. l'identità e i dati di contatto del titolare e del suo rappresentante;
2. i dati di contatto del responsabile della protezione dati;
3. le finalità del trattamento e la base giuridica;
4. gli eventuali destinatari;
5. il periodo di conservazione dei dati;
6. se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
7. i diritti di cui agli artt. da 15 a 22, riguardanti l'accesso, la rettifica, la cancellazione, la limitazione di trattamento, l'obbligo di notifica, la portabilità dei dati, l'opposizione.

Considerata la specificità della tipologia dati trattati dall'istituto scolastico e al fine di permettere il più agevole raggiungimento ed il maggiore soddisfacimento degli scopi previsti di cui agli artt.13 e 14 del Regolamento UE 2016/679, e quindi garantire agli interessati un reale, efficace e trasparente controllo del Trattamento dei dati personali che li riguardano, si è stabilito di adottare tre modelli d'informativa (redatti in base ai criteri sopra esposti): il primo rivolto agli studenti ed alle famiglie, il secondo rivolto al personale, il terzo ai fornitori. Ai fini di una maggiore diffusione, le informative sono affisse all'albo d'istituto e comunque disponibili sul sito dell'istituto e presso gli uffici di segreteria.

7.2. Esercizio dei diritti dell'Interessato

Per favorire l'esercizio dei diritti degli interessati e rispondere tempestivamente alle richieste avanzate dai medesimi, l'Istituto Scolastico ha adottato la seguente procedura.

1. **Gli interessati possono presentare le loro richieste al Titolare o al Responsabile del trattamento indicato nell'informativa;**
2. **La richiesta può essere presentata direttamente in forma orale o per iscritto, richiedendo l'apposito modulo prestampato messo a disposizione dal Responsabile presso gli uffici di segreteria ovvero a mezzo posta, per fax, per posta elettronica La predisposizione e l'uso di un modulo per l'esercizio dei diritti dell'interessato consente di definire meglio l'espressione di volontà dell'interessato, circoscrivendone l'ambito alle sole richieste indicate.**
3. **La richiesta deve essere necessariamente accolta,senza che l'interessato debba presentare le proprie motivazioni. Unico caso in cui è necessaria la motivazione riguarda l'opposizione per motivi legittimi.**
4. **La richiesta può provenire anche da una persona fisica diversa dall'interessato: in questo caso è necessario verificare la delega.**
5. **La risposta del responsabile alle richieste avanzate deve giungere senza ritardo, e comunque non oltre i tre giorni dal deposito dell'istanza.**
6. **Ai fini di controllo sulle richieste di accesso ai dati personali da parte degli interessati e sul soddisfacimento dei diritti , il responsabile del trattamento aggiorna il "Registro accessi ai dati personali".**