DOCUMENTO DI COORDINAMENTO SULLA SICUREZZA DEI DATI PERSONALI

CODICE DELLA PRIVACY

(D.Lgs. n. 196 / 2003)

D.M. n. 305 del 7.12.2006

Istituto Comprensivo Statale
"PALMIERI - S.GIOVANNI BOSCO"

Viale 2 Giugno
71016 San Severo (FG)

Revisione del 03 ottobre 2015

SOMMARIO

Riferimenti normativi

Ai fini del presente documento, si intende per:

1. **TITOLARE:** l'Istituzione scolastica rappresentata dal Dirigente Scolastico dell' **Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG)** che ha la responsabilità finale ed assume le decisioni fondamentali riferite al trattamento dei dati personali, identificativi, sensibili e giudiziari;
2. **RESPONSABILE:** persona fisica (o giuridica) nominata ai sensi dell'art. 29 del D.Lgs. 196/2003, ai quali spetta la responsabilità di qualsiasi trattamento dei dati e dotata di particolari caratteristiche di natura morale e di competenza tecnica, preposta dal titolare al trattamento dei dati personali compresa l'organizzazione della sicurezza fisica e logica delle banche dati e delle funzioni istituzionali dell' **Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG)**.
3. **INCARICATO**: persona fisica che materialmente provvede al trattamento dei dati, secondo le istruzioni impartite dal titolare o dal responsabile se nominato e che opera sotto la sua diretta autorità.
4. **INTERESSATO:** persona fisica o giuridica cui si riferiscono i dati personali e trattati dal titolare.
5. **MISURE MINIME**: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi di cui all'art. 33 del D.Lgs. 196/2003.
6. **STRUMENTI ELETTRONICI**: i mezzi elettronici o comunque automatizzati con cui è effettuato il trattamento.
7. **AMMINISTRATORI DI SISTEMA:** soggetti cui è conferito il compito di sovrintendere le risorse del sistema operativo di server o di un sistema di base dati e di consentirne l'utilizzazione.
8. **RESPONSABILE DELLA GESTIONE DELLE ABILITAZIONI:** il soggetto cui è conferito il compito di assegnare e revocare i "codici personali utenti" e le corrispondenti "parole chiave" (password).
9. **TRASMISSIONE PER VIA TELEMATICA:** trasferimento dati elettronici o documenti cartacei digitalizzati con scanner, mediante l'impiego di FAX, la compilazione di form in applicativi on line via Internet, l'impiego di applicativi di gestione dati personali on line amministrati da organizzazioni esterne, l'impiego di software.
10. **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" art. 4 c. 2 D. Lgs. 196/03

In ottemperanza al1'art. 31 del D.Lgs. n. 196 del 30.06.2003 i dati personali oggetto di trattamento, devono essere custoditi e controllati, 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, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

In ottemperanza all'art. 34 D.Lgs. n. 196 del 30.06.2003 il trattamento di dati sensibili mediante strumenti elettronici, deve essere effettuato in base alle misure minime previste dal disciplinare tecnico contenuto nell'allegato B) della legge stessa. **Si ritiene pertanto necessario, per un migliore coordinamento delle attività poste in essere a tutela dei dati personali trattati nell'Istituto, predisporre e mantenere aggiornato il presente "Documento di Coordinamento delle attività sulla sicurezza dei dati personali", finalizzato alla definizione delle misure di sicurezza necessarie sulla base dell'analisi dei rischi, dell'attribuzione dei compiti e delle responsabilità deputate al trattamento dei dati stessi**. In particolare il presente DCS si propone di descrivere e programmare:

Le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

- La descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- La previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati.

Ambito di applicazione

Il presente documento, nell'ambito delle attività svolte presso l' **Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG)**, in riferimento alle misure di sicurezza previste dall'art. 33 della D.Lgs. n.196/03 e agli standard minimi esposti nell'Allegato B del D.Lgs. stesso, intende definire gli elementi di riferimento necessari per l'adozione, l'adeguamento, lo sviluppo, l'implementazione gestionale di misure di sicurezza relative a:

- Trattamento dei dati personali comuni (riferiti a dati senza particolare rilevanza caratteristica)
- Trattamento dei dati sensibili definiti all'art. 4 comma 1 lettere d) ed e), con riguardo a quanto previsto dagli art. 34 e 35 del D.Lgs. n. 196/2003;
- Gestione di archivi cartacei (correnti, di deposito, storici) e di banche dati conservate su supporti informatizzati-automatizzati (LAN, WAN, hard-disk, floppy disk, cd-rom, drive usb, ecc.);

- Gestione di archivi contenenti documenti particolari.

Trattamento dei dati mediante strumenti elettronici

Le misure di sicurezza previste nel presente documento, si applicano alle procedure gestite dal personale incaricato presso l' **Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG)**.

Il rappresentante del titolare o i responsabili, nominati ai sensi dell'art. 29 del D.Lgs. 196/2003, provvedono per iscritto alla nomina dei soggetti incaricati, da abilitarsi all'uso delle procedure informatizzate, specificando per ciascuno a quali funzioni/insiemi di dati devono essere in grado di accedere. Il rappresentante del titolare o i responsabili, con le medesime modalità, impartiscono agli incaricati le necessarie istruzioni per il corretto utilizzo di dette procedure. Il rappresentante del titolare o i responsabili della gestione delle abilitazioni provvedono a svolgere i propri compiti con le seguenti modalità:

- A ciascun incaricato che, per esigenze di servizio, deve poter utilizzare una procedura informatizzata ed accedere di conseguenza alle informazioni contenute negli archivi della stessa, è assegnato un "codice personale utente" ed una "parola chiave" segreta (password) individuale e riservata in modo esclusivo.
- Ciascun incaricato, per mezzo di detto codice di accesso, è abilitato all'utilizzo delle funzionalità necessarie allo svolgimento delle attività allo stesso assegnate e può contemporaneamente accedere ai soli dati strettamente necessari allo scopo.
- Ciascuna procedura informatizzata deve essere strutturata in modo da consentire di adottare dei livelli di abilitazione di accesso ed utilizzo delle basi dati.
- Ciascun incaricato ha l'obbligo di non comunicare ad altri il proprio codice identificativo personale, né la parola chiave (password) segreta, di non lasciare la stazione di lavoro situata al proprio posto di lavoro collegata ed incustodita, di non utilizzare i dati consultabili per fini non strettamente attinenti alle esigenze di servizio.

Trattamento dei dati mediante strumenti non elettronici

Il rappresentante del titolare del trattamento o i responsabili, ai sensi dell'art. 30 del D.Lgs. n. 196/2003, devono delineare per iscritto e consegnare agli incaricati, le istruzioni descriventi le modalità e i limiti di accesso ai dati personali la cui conoscenza sia strettamente necessaria per adempiere i compiti loro assegnati. Tutti gli atti, i documenti, le procedure, i fascicoli contenenti i dati devono essere conservati in archivi ad accesso controllato e selezionato e devono essere restituiti o conservati al termine delle operazioni eseguite. In particolare per quanto attiene il trattamento dei dati sensibili o di natura giudiziaria, con riferimento a quanto indicato

agli art. 4 comma 1 lettere d) ed e) del D.Lgs. n. 196/2003, gli incaricati conserveranno gli atti, i documenti, le procedure e i fascicoli **in contenitori muniti di serratura**.

Le medesime modalità si applicano alla conservazione anche dei supporti non informatici contenenti la riproduzione di informazioni relative al trattamento dei dati.

Ulteriori regole e procedure relative alle modalità di trattamento saranno trattate in seguito.

Premessa

Nel presente documento sono esposte le misure di sicurezza individuate per l' **Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG)** in ottemperanza a quanto disposto dall'art. 22 del D.Lgs. n. 196/2003 "Principi applicabili al trattamento di dati sensibili e giudiziari" relativi al Capo II "REGOLE ULTERIORI PER I SOGGETTI PUBBLICI" ed al ***"REGOLAMENTO"*** emanato dal MPI **(**D.M. n. 305 del 7.12.2006**)** concernente **l'*"identificazione dei dati sensibili e giudiziari trattati dal MPI* e dalle Istituzioni Scolastiche**". Lo scopo è quello di delineare le misure minime di sicurezza, come indicato nel disciplinare tecnico contenuto nell'allegato B) del D.Lgs. n. 196/2003.

Il trattamento dei dati è effettuato secondo specifiche competenze dai docenti, dal personale ATA, dal Direttore Amministrativo, dal Dirigente Scolastico.

Titolare

Per tutti i trattamenti effettuati presso l' **Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG)**, in conformità a quanto previsto dall'art. 4 del D.Lgs. n. 196/03, il Titolare è l' **Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG)**, legalmente rappresentato dal Dirigente Scolastico, **Prof.ssa Francesca CHIECHI.**

Responsabili del trattamento

In conformità a quanto previsto dal D.Lgs. n. 196/2003 viene nominato, in qualità di Responsabile per i trattamenti dei dati che riguardano in modo specifico i servizi di segreteria e di amministrazione, il **Direttore dei Servizi Generali ed Amministrativi**, mentre il **Dirigente Scolastico** mantiene la diretta responsabilità per i trattamenti effettuati da docenti e dal restante personale con i dati personali di alunni e famiglie. **Il direttore amministrativo, NARDELLA Lucia**, è nominato quale *Responsabile* dal titolare del trattamento con lettera di incarico, controfirmata per accettazione. Copia della lettera di incarico va conservata dal titolare del trattamento in luogo sicuro.

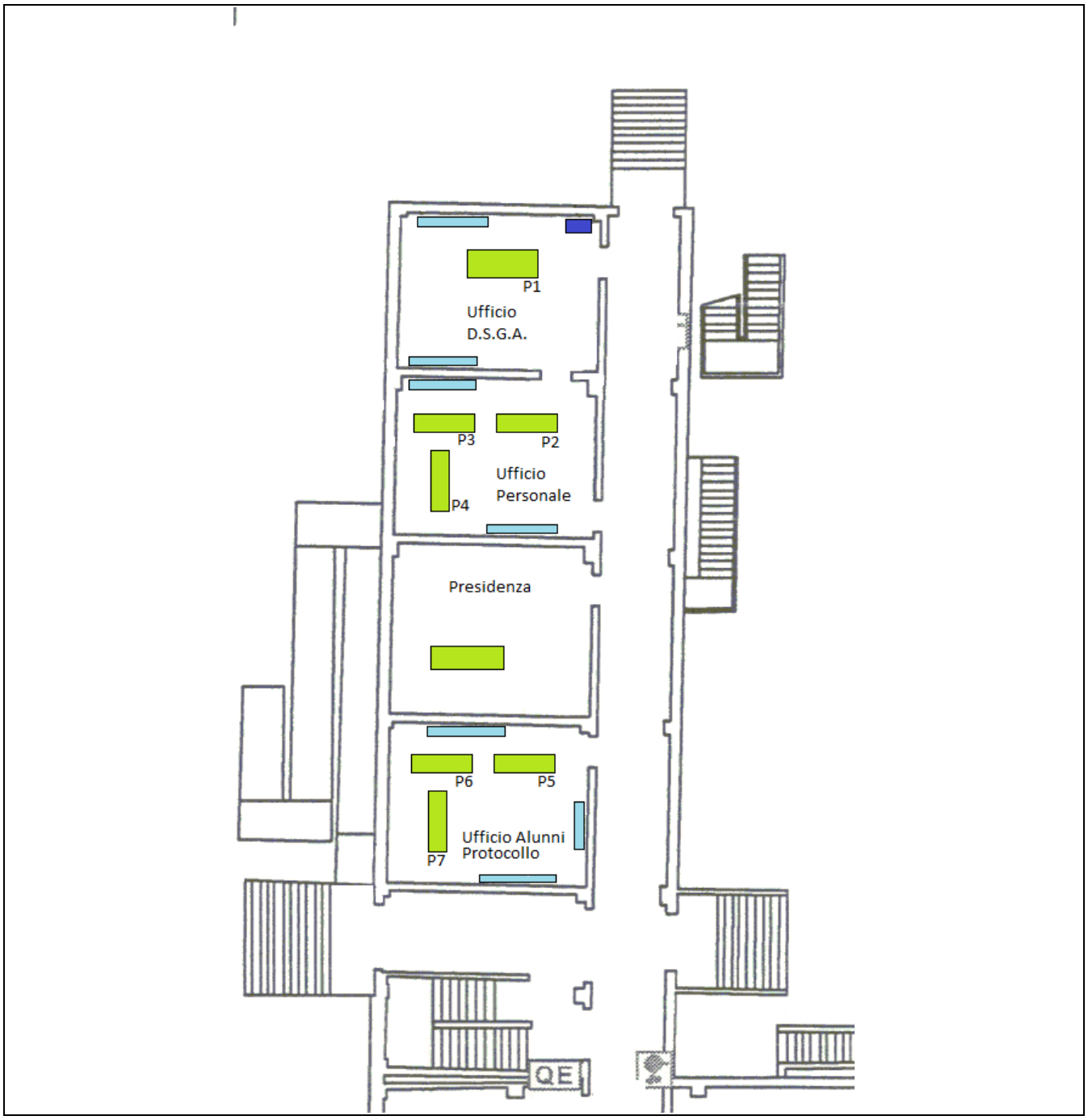
Analisi della situazione del Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG)

L'Istituzione scolastica è attualmente composta dalla sede centrale di **Viale 2 Giugno**, presso la quale sono ubicati gli uffici amministrativi e la dirigenza scolastica, e da **n. 3 sedi distaccate**. Precisamente:

PRIMARIA	Via Alfieri - San Severo (FG)
INFANZIA	Via Don Minzoni - San Severo (FG)
PRIMARIA/INFANZIA	Via Marconi - San Severo (FG)

Trovandosi gli uffici amministrativi e la dirigenza scolastica ubicati presso la sede centrale di **Viale 2 Giugno**, tutti i trattamenti di dati personali sono svolti presso la medesima sede, dove pure sono fisicamente conservate le banche dati.

In seguito si riportano i dettagli e le caratteristiche dei locali adibiti ad Uffici amministrativi:



PIANTA PIANO Rialzato – Zona Uffici

- Sistema antifurto e antintrusione: Si, con rilevatori volumetrici.
- Sistema antincendio: estintori per emergenze
- **La sede non ha custode.**

Tabella 1 - Locali ed uffici:

ID locale	*Descrizione*	*Apparecchiature elettroniche, archivi presenti (vedi allegato 2)*
1.2	Ufficio Dirigente Scolastico	1 PC impiegato dal Dirigente Scolastico **collegato alla rete internet ed intranet d'istituto**, stampante, protocollo riservato, valutazioni circa l'idoneità del personale, attività sindacali, armadi contenti documenti con dati comuni. ▪ sistema antifurto e antintrusione: si ▪ sistema antincendio: no ▪ durante il periodo di inattività: l'ufficio è chiuso a chiave
1.3	Ufficio DSGA	1 PC collegato alla rete di amministrazione, 1 stampante, mobili con serratura contenenti atti amministrativi con dati comuni e sensibili, cd e supporti cartacei con relazioni dei consigli d'istituto e GE, backup ARGO-SIDI ▪ sistema antifurto e antintrusione: si ▪ sistema antincendio: no ▪ durante il periodo di inattività: l'ufficio è chiuso a chiave
1.4	Ufficio Personale	N. 3 PC collegati alla rete amministrativa con gestione ARGO-SIDI, armadi di sicurezza contenenti fascicoli personale con dati comuni e sensibili relativi, documenti contabili, n. 2 stampanti. ▪ sistema antifurto e antintrusione: si ▪ sistema antincendio: no ▪ durante il periodo di inattività: l'ufficio è chiuso a chiave
1.5	Ufficio Alunni e Protocollo	N. 3 PC collegati alla rete amministrativa con gestione ARGO-SIDI, armadi di sicurezza contenenti fascicoli alunni con dati comuni e sensibili relativi, n. 1 stampanti. ▪ sistema antifurto e antintrusione: no ▪ sistema antincendio: si ▪ durante il periodo di inattività: l'ufficio è chiuso a chiave
1.6	Sala Server	Locale situato al primo piano dell'edificio scolastico, dedicato alla collocazione del server dell'area amministrativa. **In tale locale è presente il Server (database ARGO-SIDI) collegato alla rete amministrativa** ▪ sistema antifurto e antintrusione: si ▪ sistema antincendio: no ▪ durante il periodo di inattività: l'ufficio è chiuso a chiave

Altri locali, aule e laboratori allo stato attuale sono impiegati esclusivamente per fini legati alla didattica e pertanto sono da reputare ininfluenti rispetto al trattamento dei dati personali descritti nel presente documento.

- *Sedi distaccate:*

Sono deputate esclusivamente ad attività didattiche senza nessuna archiviazione di dati comuni o sensibili, ad eccezione dei registri dei docenti e di classe che sono raccolti a fine giornata e conservati in apposito vano chiuso a chiave a cura dei collaboratori scolastici.

Tabella 2 – Elenco dei trattamenti

ELENCO DEI TRATTAMENTI: INFORMAZIONI BASE								
Id	**Descrizione sintetica**	**Natura dati trattati**		**Struttura di riferimento e incaricati**	**Altre strutture (anche esterne) che concorrono al trattamento**	**Descrizione degli strumenti utilizzati**	**Eventuale banca dati**	**Ubicazione fisica dei supporti di memorizzazione**
		Sens.	Giud.					
T1	Dati di alunni trattati da docenti	X		Corpo docenti	Dirigenza Scolastica, Direzione amministrativa, Collaboratori	non elettronici	\	\
T2	Dati alunni trattati da Assistenti amministrativi e DSGA	X	X	Direzione amministrativa	Dirigenza Scolastica	Elaboratori elettronici	SISSI-SIDI, archivi doc. elettronici negli elaboratori	Server, P1, P5, P6, P7
T3	Personale dipendente	X	X	Direzione amministrativa	Dirigenza Scolastica,	Elaboratori elettronici	SISSI-SIDI, archivi doc. elettronici negli elaboratori	Server, P1, P2, P3, P4

ELENCO DEI TRATTAMENTI: INFORMAZIONI BASE

Id	Descrizione sintetica	Natura dati trattati		Struttura di riferimento e incaricati	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione
		Sens.	Giud.					
T4	Collaborazioni professionali esterne	X		Direzione amministrativa	Dirigenza Scolastica,	Elaboratori elettronici	SISSI-SIDI, archivi doc. elettronici negli elaboratori	Server,
T5	Beni e servizi: acquisti, affitti, vendite	X		Direzione amministrativa	Dirigenza Scolastica,	Elaboratori elettronici	SISSI-SIDI, archivi doc. elettronici negli elaboratori	Server
T6	Gestione finanziaria e del bilancio	X		Direzione amministrativa	Dirigenza Scolastica,	Elaboratori elettronici	SISSI-SIDI, archivi doc. elettronici negli elaboratori	Server, P1

ELENCO DEI TRATTAMENTI: INFORMAZIONI BASE

Id	Descrizione sintetica	Natura dati trattati		Struttura di riferimento e incaricati	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati	Eventuale banca dati	Ubicazione fisica dei supporti di memorizzazione
		Sens.	Giud.					
T7	Gestione Istituzionale, Protocollo e Posta	X		Direzione amministrativa	Dirigenza Scolastica,	Elaboratori elettronici	Posta elettronica, doc. elettronici negli elaboratori	Server, P7
T8	Gestione di dati personali di soggetti anche esterni alla scuola, facenti parte degli organi collegiali	X		DS: consigli di classe, collegio docenti; DSGA: GE, CDI;	Direzione amministrativa Dirigenza Scolastica	Elaboratori elettronici e non	\	//
T9	Gestione Trattamenti di dati personali effettuati da Collaboratori Scolastici e Personale Ausiliario	X		Collaboratori Scolastici e Personale Ausiliario	Direzione amministrativa Dirigenza Scolastica	non elettronici	\	

ELENCO DEI TRATTAMENTI: INFORMAZIONI BASE								
Id	**Descrizione sintetica**	**Natura dati trattati**		**Struttura di riferimento e incaricati**	**Altre strutture (anche esterne) che concorrono al trattamento**	**Descrizione degli strumenti utilizzati**	**Eventuale banca dati**	**Ubicazione fisica dei supporti di memorizzazione**
		Sens.	Giud.					
T10	Gestione e amministrazione informatica degli strumenti e degli archivi elettronici, dei sistemi di sicurezza informatica, autenticazione autorizzazione cifratura	X	X	Amministratore di sistema	Direzione amministrativa Dirigenza Scolastica	Elaboratori elettronici	Tutte	Server

Sistemi Informatici

Allo stato attuale l'istituzione scolastica si avvale di elaboratori (EL) composti da PC Desktop per la gestione di dati informatici collegati in rete locale. In particolare i dati trattati con strumenti elettronici sono gestiti secondo il seguente schema:

Tabella 3 – Postazioni di lavoro, strumenti e archivi.

Post	PC	Archivi fisici	Postazione	Tipo Elaboratore	Sistema operativo	Software utilizzato	Rete	Archivi accessibili (Tab.4)	Figura incaricata
Server	EL00		*Sala server*	Intel Pentium 4	S.O. Windows Server 2003	Gestionale ARGO-SIDI, Office 2007, Antiv. Avast	LAN1	Tutti	PERNA ANTONIO
P.1	EL01	Annessi	*Uff. DSGA*	Pentium Dual Core	S.O. Windows 7 Prof.	Gestionale ARGO-SIDI, Office 2007, Antiv.Avast	LAN1	Tutti	D.S.G.A (NARDELLA LUCIA)
P.2	EL02	Annessi	*Uff. Personale*	Intel Core 2 Duo	S.O. Windows 7 Prof.	Gestionale ARGO-SIDI, Office 2007, Antiv.Avast	LAN1	Personale	PONTONIO TOMMASO
P.3	EL03	Annessi	*Uff. Personale*	Pentium Dual Core	S.O. Windows 7 Prof.	Gestionale ARGO-SIDI, Office 2007, Antiv.Avast	LAN1	Personale	MARCHESANI COSTANZO
P.4	EL04	Annessi	*Uff. Personale*	Pentium 4	S.O. Windows XP Prof.	Gestionale ARGO-SIDI, maRCATEMPO, Office 2007, Antiv.Avast	LAN1	Personale, Magazzino acquisti	BISCOTTI LUIGI
P.5	EL05	Annessi	*Uff. Alunni E Protocollo*	Pentium D	S.O. Windows XP Prof.	Gestionale ARGO-SIDI, Office 2007, Antiv.Avast	LAN1	Alunni, Inventario	PERNA ANTONIO
P.6	EL06	Annessi	*Uff. Alunni E Protocollo*	Pentium Dual Core	S.O. Windows 7 Prof.	Gestionale ARGO-SIDI, Office 2007, Antiv.	LAN1	Alunni	SORDILLO GIUSEPPINA
P.7	EL07	Annessi	*Uff. Alunni E Protocollo*	Pentium Dual Core	S.O. Windows 7 Prof.	Gestionale ARGO-SIDI, Office 2007, Antiv.	LAN1	Protocollo, Posta elettronica	DE ROSA GIUSEPPINA

- *Reti locali e sottorete di amministrazione LAN1*:

- LAN distribuita negli uffici amministrativi e dirigenziali. È presente un sistema di protezione informatica per il controllo degli accessi interni ed esterni degli archivi elettronici e dei dispositivi di elaborazione elencati ai punti precedenti. La connessione ADSL è di tipo permanente con indirizzo IP statico pubblico. Il servizio Internet è consentito a tutte le unità di accesso. La rete LAN è suddivisa in sottorete di amministrazione e sottorete di didattica, ognuna delle quali è gestita autonomamente dal punto di vista della sicurezza informatica.

Figure attive e organigramma

L'attuazione del trattamento dei dati personali avviene in forma cartacea o elettronica come indicato nel D.Lgs. 196/03, in relazione alle modalità di raccolta, di trattamento, di conservazione e di comunicazione o diffusione dei dati stessi. Le operazioni di trattamento coinvolgono diverse tipologie di soggetti e prevedono la figura di "incaricato" in servizio presso l' **Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG)**.

Il trattamento dei dati per via elettronica avviene utilizzando software di gestione operante nei PC indicati nella sezione precedente, oppure mediante produzione di documenti per mezzo di Microsoft Office. Tutte le altre procedure di trattamento dei dati avvengono utilizzando strumenti non elettronici.

I dettagli relativi al trattamento dei dati sono riportati nell'allegato 1 del presente documento.

In seguito saranno descritti le procedure da attuare da parte degli incaricati al trattamento dei dati e delle funzioni assegnate.

Le figure coinvolte nel trattamento dei dati sono:

- **Dirigente scolastico**
- **Direttore dei Servizi Generali e Amministrativi (DSGA)**
- **Docenti**
- **Assistenti Amministrativi**
- **Membri degli Organi Collegiali**
- **Personale e collaboratori scolastici**
- **Amministratore di rete**

In seguito sono riportati in forma sintetica le modalità di trattamento e le

relative procedure di ogni figura rimandando per i dettagli agli allegati 1 e 3.

- ***Dirigente Scolastico***. Ha piena facoltà nel trattare qualunque tipo di dati, sia mediante strumenti elettronici, sia senza l'ausilio di strumenti elettronici. In particolare il Dirigente Scolastico tratta alcuni dati personali caratterizzati da specifica riservatezza. È facoltà del Dirigente Scolastico di avvalersi di collaboratori o del DSGA per il trattamento di tali dati personali. Rimandando i dettagli all'allegato 1) del presente documento i dati trattati nella circostanza dal Dirigente Scolastico sono:

  - Dati sensibili relativi agli alunni diversamente abili. Tali dati sono conservati in appositi archivi come indicato nell'allegato 2 ovvero secondo le disposizioni del Dirigente Scolastico anche nella cassaforte della Dirigenza Scolastica. I documenti cartacei ed elettronici contenente tali dati possono essere raccolti anche da un collaboratore del dirigente che consegna gli stessi in busta chiusa o utilizzando strumenti elettronici conformi alle misure minime previste in questo documento, al Dirigente Scolastico che prenderà decisioni sulle modalità di trattamento e sulla conservazione dei dati.
  - Protocollo riservato: il Dirigente Scolastico provvede a protocollare documenti contenenti dati di particolare riservatezza. I documenti protocollati vengono passati all'Incaricato che deve trattare la pratica, che si occupa anche dell'archiviazione o della spedizione. Documenti di valenza istituzionale perpetua o pluriennale sono archiviati a parte. Sono soggetti allo stesso trattamento del protocollo riservato anche i documenti cartacei prodotti mediante trasmissione per via telematica (fax, posta elettronica, ecc.).
  - Fascicoli del personale docente, amministrativo e collaboratori: tali dati sono trattati in stretta collaborazione con il DSGA quale responsabile dei dati relativi all'Amministrazione. I dati raccolti sono trattati normalmente dal DSGA e dagli assistenti amministrativi seguendo le regole descritte nell'allegato1.
  - Documenti contabili, contratti di fornitura e di acquisto. Tali dati sono trattati in stretta collaborazione con il DSGA quale responsabile dei dati relativi all'Amministrazione. I dati raccolti sono trattati normalmente dal DSGA e dagli assistenti amministrativi seguendo le regole descritte nell'allegato1.
  - Dati dipendenti relativi ad attività sindacali: tali dati sono trattati direttamente dal Dirigente Scolastico e dai suoi collaboratori. I dati sono raccolti direttamente dai membri o dagli organizzatori dell'attività sindacale e consegnati per conoscenza al Dirigente Scolastico. Gli stessi dati possono essere trasmessi anche ad organizzazioni di competenza esterne come indicato nell'allegato 1 del presente documento.

- ***DSGA*** In qualità di responsabile della gestione amministrativa dell'

Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG) ha la facoltà di trattare qualunque tipo di dato personale inerenti le attività amministrative. Come regola generale il DSGA si avvale della collaborazione degli assistenti amministrativi ai quali affiderà specifici compiti relativi alle modalità di trattamento e di conservazione dei dati. Tali dati saranno trattati con strumenti cartacei o elettronici utilizzando in particolare le funzioni del software ARGO**-SIDI**. Il DSGA provvederà ad informare i propri incaricati e trattare i dati con particolare riserbo evitando il rischio di divulgazioni accidentali o intenzionali. In seguito si elencano le categorie di dati personali trattati dal DSGA rimandando all'allegato 1 per ulteriori particolari.

- attività amministrative, inerenti la didattica e integrative
- stati personali e familiari riservati
- assicurazione, infortuni, denuncie, compresa eventuale applicazione D.Lgs. 81/2008
- dati dipendenti e loro famiglie per l'attività amministrativa
- dati dipendenti e loro famiglie relativi alla retribuzione, previdenza
- dati dipendenti per le attività riguardanti la didattica
- dati dipendenti relativi a pratiche di assicurazione, gestione infortuni e malattie professionali, di inabilità al lavoro e simili
- dati dipendenti relative ad attività sindacali salvo particolari disposizioni del Dirigente Scolastico
- dati dei collaboratori esterni per l'attività amministrativa, retributiva, previdenziale, fiscale e tutti gli altri ARGOmenti connessi alla categoria
- protocollo ordinario
- dati contenuti prodotti con Microsoft Office
- database relativi a tutte le aree delle procedure ARGO**-SIDI**

- ***Assistenti amministrativi***. sono incaricati direttamente dal DSGA quale responsabile del trattamento dei dati relativi all'Amministrazione. Il personale di amministrazione ha il compito principale di trattare dati gestiti nelle aree delle procedure ARGO-SIDI e dati su supporto cartaceo. In particolare il personale può accedere alle aree di propria competenze mediante funzioni di discriminazione degli accessi. Oltre al trattamento dei dati con strumenti elettronici il personale di amministrazione accede alle categorie di dati personali elencati al punto precedente.

- ***Docenti.*** Sono incaricati direttamente dal Dirigente Scolastico il quale provvede a disporre le modalità di trattamento dei dati personali con particolare riguardo a quelli caratterizzati da un elevato grado di sensibilità come i dati relativi allo stato di salute. I docenti sono autorizzati al trattamento dei dati personali degli alunni limitatamente alle informazioni inerenti l'attività didattica. Attualmente i docenti effettuano i trattamenti dei dati senza l'ausilio di strumenti elettronici con

particolare riferimento alle seguenti categorie di dati:

Didattica e attività correlate: dati generalmente contenuti in registri ed elaborati

- Handicap, stato di salute: in particolare solo i docenti di sostegno sono incaricati al trattamento di questa categoria di dati utilizzando anche strumenti elettronici. Tali dati saranno trattati su disposizione del Dirigente Scolastico.

- ***Membri degli Organi Collegiali:*** sono incaricati direttamente dal Dirigente Scolastico. I membri sono composti da docenti, alunni e genitori che possono accedere a notizie riguardanti dati personali anche sensibili. Il Dirigente Scolastico provvede a fornire le informazioni sul trattamento dei dati di competenza dei membri. I dati trattati dai membri degli Organi Collegiali consistono in atti e delibere riguardanti persone interne o esterne quali fornitori di beni e servizi. I documenti saranno conservati in appositi archivi come indicato nell'allegato 2 del presente documento

- ***Personale e collaboratori scolastici:*** sono incaricati direttamente dal Dirigente Scolastico o dal D.S.G.A.. I dati trattati sono normalmente dati comuni o contenuti in buste chiuse se trattasi di dati riservati. Le modalità di trattamento sono inerenti le normali procedure di raccolta dei documenti in ingresso e in uscita da svolgere in collaborazione con altri incaricati quali il DSGA e gli assistenti amministrativi. Essi possono: ricevere, trasportare, consegnare, inviare documenti contenenti dati comuni o sensibili collocati in busta chiusa o aperta, tra cui registri; visionare documenti contenenti dati comuni al solo scopo di dare indicazioni di massima agli utenti; custodire documenti e registri per brevi periodi; gestire dati comuni in elenchi di alunni, dipendenti e genitori per attività varie della scuola; effettuare fotocopie e fax di documenti contenenti dati comuni; collaborare ad operazioni di archiviazione di documenti cartacei; collaborare ad operazioni di scarto ed eliminazione di documenti cartacei; in generale, svolgere attività di supporto a tutti i trattamenti svolti nella scuola

- ***Amministratore di rete:*** qualora incaricato, assume il compito della gestione di tutti gli strumenti informatici trattanti dati personali contenuti negli archivi elettronici. L'amministratore di rete assume il compito di controllo dei sistemi di sicurezza informatici, di autenticazione, autorizzazione e cifratura intervenendo direttamente in seguito alla rilevazione di malfunzionamenti, operazione di configurazione o su chiamata da parte dell'interessato.

Organigramma del trattamento e responsabilità

Le strutture di riferimento in cui sono effettuati il trattamento dei dati sono gestite dalle figure previste agli art. 28-30 del D.Lgs. 196/2003. Per responsabile della struttura si intende il ruolo o la qualifica del dirigente o del responsabile della struttura stessa che non necessariamente coincide con il responsabile del trattamento ai sensi dell'art. 29 del D.Lgs. 196/2003.

NOMINATIVO	RUOLO	FIGURA
CHIECHI FRANCESCA	**DIRIGENTE SCOLASTICO**	**TITOLARE (Legale Rappresentante)**
NARDELLA LUCIA	**D.S.G.A.**	**RESPONSABILE AREA AMMINISTRATIVA**
NARDELLA LUCIA	**D.S.G.A.**	**CUSTODE DELLE PASSWORD**

Il Titolare

Il titolare del trattamento, come già indicato, è l' Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG), legalmente rappresentato dal Dirigente Scolastico Prof.ssa Francesca CHIECHI. I compiti che il titolare ha l'obbligo di svolgere sono:

- Eventuali notifiche al garante
- Scelte sulle modalità di raccolta e verifica dei dati
- Controllo dell'informativa da consegnare all'interessato
- Controllo dei dati sensibili ed eventuali autorizzazioni
- Controllo delle idonee misure di sicurezza
- Controllo della applicazione del D.Lgs. 196/2003 da parte dei soggetti preposti

Il responsabile del trattamento dei dati amministrativi adempie alle procedure relative ai dati trattati con procedure elettroniche e non elettroniche.

Gli incaricati al trattamento dei dati sono le figure già individuate nel presente documento ed elencati nella tabella 3. Ad essi vanno aggiunte tutte le altre figure che potranno essere coinvolte al trattamento qualora trattino anche saltuariamente dati personali. Gli incaricati del trattamento dei dati inerenti l'amministrazione sono nominati dal responsabile, mentre lo stesso responsabile e tutte le altre figure sono nominate dal titolare del trattamento con lettera di incarico controfirmata dall'interessato per accettazione. Copia della lettera di incarico va conservata dal titolare del trattamento in luogo sicuro. Gli incaricati sono identificabili in classi con caratteristiche omogenee delle tipologia del trattamento come di seguito esposto.

D.S.G.A.

Il D.S.G.A. è il responsabile del trattamento dei dati riguardanti l'Amministrazione dell'Istituzione Scolastica e dispone le funzioni da affidare agli assistenti amministrativi. Per tale soggetto valgono le seguenti procedure (si veda l'allegato 2 per i dettagli):

- PPD00

Per il trattamento manuale o con strumenti non elettronici:

- Da PPD01 a PPD12, PPD19, PPD21, PPD22

Per il trattamento con strumenti elettronici:

- Da PPD13 a PPD17

Assistente amministrativo

Gli assistenti amministrativi svolgeranno il trattamento dei dati relativamente alle funzioni svolte in ufficio secondo le disposizioni del responsabile del trattamento (DSGA).

Le categorie di dati trattati di loro competenza sono individuate nella **Tabella 2**. Per essi valgono le seguenti regole (allegato 2):

- PPD00

Per il trattamento manuale o con strumenti non elettronici:

- Da PPD01 a PPD12, PPD19, PPD21, PPD22

Per il trattamento con strumenti elettronici:

- Da PPD13 a PPD17

Collaboratori del Dirigente Scolastico

I collaboratori del dirigente scolastico hanno il compito di trattare dati personali secondo le disposizioni del titolare come ausilio alle procedure di trattamento. In base a tale incarico i collaboratori assumono alcuni degli incarichi del Dirigente Scolastico. Pertanto valgono le stesse regole assunte dal Dirigente Scolastico

Docenti

I docenti sono considerati incaricati del trattamento dei dati relativamente alle categorie di loro competenza individuate nella **Tabella 2** e sono nominati dal

Dirigente Scolastico. Per loro valgono le seguenti regole specifiche (allegato 2):

- PPD00

Per il trattamento manuale o con strumenti non elettronici:

- Da PPD18 a PPD22

Per il trattamento con strumenti elettronici:

- nessuno

Membri Organi Collegiali

I membri degli organi collegiali sono nominati dal Dirigente scolastico ed hanno il compito di trattare i dati personali scaturiti dagli Organi Collegiali. Tali dati sono generalmente contenuti in verbali e delibere prodotti dal Consiglio di Istituto anche utilizzando programmi di Office (Microsoft Office). Per tali figure valgono le seguenti regole (allegato 2):

- PPD00

Per il trattamento manuale o con strumenti non elettronici:

- PPD23

Per il trattamento con strumenti elettronici:

- nessuno

Collaboratori Scolastici e Personale Ausiliario

I collaboratori scolastici, dovranno essere nominati dal titolare del trattamento con lettera di incarico controfirmata dall'interessato, indicando le regole e il tipo di dati che potranno trattare. Copia della lettera di incarico va conservata dal titolare del trattamento in luogo sicuro.

Per tali figure valgono le seguenti regole secondo le loro competenze (allegato 2):

- PPD00

Per il trattamento manuale o con strumenti non elettronici:

- PPD01, PPD09, PPD10, PPD11, PPD12, PPD22, PPD24, PPD25, PPD26

Per il trattamento con strumenti elettronici:

- nessuno

Amministratore di sistema

L'Amministratore di sistema, qualora nominato, ha il compito di garantire la funzionalità ed il corretto uso dei sistemi informatici descritti al punto 8.1. Particolare attenzione si dovrà prestare al sistema di protezione informatico. Pur non definito esplicitamente nel D.Lgs. 196/2003 il suo compito è quello di controllare e monitorare le risorse dei server e degli applicativi software compreso i sistemi di base dati.

Le attribuzioni dei ruoli e la definizione dettagliata dei compiti e delle modalità operative assegnate sono (allegato 2):

- PPD00

Per il trattamento manuale o con strumenti non elettronici:

- nessuno

Per il trattamento con strumenti elettronici:

- Da PPD013 a PPD017

La Tabella 3 riassume le strutture organizzative dell' **Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG)** relativamente al trattamento dei dati.

Tabella 4 – Strutture preposte al trattamento:

STRUTTURE PREPOSTE AL TRATTAMENTO			
Struttura	Responsabile della struttura	Trattamenti operati	Compiti della struttura

STRUTTURE PREPOSTE AL TRATTAMENTO			
Struttura	Responsabile della struttura	Trattamenti operati	Compiti della struttura
Dirigenza Scolastica	Dirigente Scolastico	Tutti Protocollo riservato	Scelte sulle modalità di raccolta e verifica dei dati Controllo e assegnazione agli incaricati modalità di trattamento di tutti i dati personali Controllo dell'informativa da consegnare all'interessato Controllo dei dati sensibili ed eventuali autorizzazioni Controllo delle idonee misure di sicurezza Controllo della applicazione del D.LGS. 196/2003 da parte dei soggetti preposti

STRUTTURE PREPOSTE AL TRATTAMENTO			
Struttura	Responsabile della struttura	Trattamenti operati	Compiti della struttura
Direzione Amministrativa	DSGA	attività amministrativa e altre attività correlate, attività inerenti la didattica, attività integrative origine etnica e religiosa, stati personali e familiari riservati, assicurazione, infortuni, denuncie, compresa eventuale applicazione D.Lgs 81/08, dati dipendenti e loro famiglie per l'attività amministrativa, dati dipendenti e loro famiglie relativi alla retribuzione, previdenza, dati dipendenti per le attività riguardanti la didattica, dati dipendenti relativi a pratiche di assicurazione, gestione infortuni e malattie professionali di inabilità al lavoro e simili, dati dipendenti relative ad attività sindacali, dati dei collaboratori esterni per l'attività amministrativa, retributiva, previdenziale, fiscale e tutti gli altri ARGOmenti connessi alla categoria, dati amministrativi, fiscali e tutti gli altri ARGOmenti connessi alla gestione dei beni e servizi, dati connessi alla gestione del programma annuale e tutti gli ARGOmenti connessi, compresi i rapporti con le banche. Protocollo ordinario Affari generali	Trattamento dei dati con mezzi elettronici, e non elettronici delle procedure inerenti l'Amministrazione, gli alunni, il personale dipendente, collaborazioni esterne, beni e servizi, finanza e bilancio, protocollo e posta.

STRUTTURE PREPOSTE AL TRATTAMENTO			
Struttura	Responsabile della struttura	Trattamenti operati	Compiti della struttura
Assistenti Amministrativi	DSGA	Dati della direzione amministrativa secondo le disposizioni del DSGA	Trattamento dei dati con mezzi elettronici, e non elettronici delle procedure, secondo le disposizioni del DSGA inerenti l'Amministrazione, gli alunni, il personale dipendente, collaborazioni esterne, beni e servizi, finanza e bilancio, protocollo e posta.
Collaboratori del Dirigente Scolastico	Dirigenza Scolastica	Dati specifici trattati secondo le disposizioni del Dirigente Scolastico	Collaborazione con il Dirigente Scolastico per il trattamento di alcuni dati specifici
Docenti	Dirigenza Scolastica	didattica e attività correlate, Handicap, stato di salute	Trattamento dei dati personali degli alunni inerenti la didattica
Membri Organi Collegiali	D.S.G.A.	delibere e atti del CdI e GE	Atti e delibere riguardanti persone interne o esterne quali fornitori di beni e servizi
Collaboratori Scolastici e Personale Ausiliario	D.S. e D.S.G.A.	Dati comuni di alunni, docenti, personale della scuola contenuti in qualunque tipologia di documenti anche in collaborazione con altri incaricati	Apertura e chiusura della sede, custodia e controllo, consegna e ricezione plichi e lettere, pulizia, assistenza a tutte le altre attività
Amministratore di sistema	Dirigente Scolastico	Dati comuni e sensibili degli archivi elettronici, chiavi di autenticazione, crittografia, password, credenziali di autenticazione	Interventi sui sistemi elettronici contenenti dati personali. Produzioni di parole chiave, password, credenziali di autenticazione e chiave di crittografia

Analisi dei rischi che incombono sui dati

Gli eventi potenzialmente dannosi per la sicurezza dei dati sono valutabili in funzione delle gravità delle conseguenze rispetto alle quali dovranno essere intraprese adeguate misure di prevenzione.

Gli eventi di rischio possono derivare da:

- azioni intenzionali o accidentali causate dal personale interno
- azioni intenzionali da parte di personale esterno
- software dannosi introdotti in rete o su singole unità di accesso
- eventi accidentali dovute a cause naturali.

Gli eventi di rischio sono classificabili in:

- comportamenti errati da parte degli operatori (titolare, responsabile, incaricati) al trattamento
- eventi che agiscono sugli apparati di automazione della gestione dei dati
- eventi relativi al contesto fisico degli ambienti in cui sono posti i dati.

Comportamenti errati da parte degli operatori

Gli operatori che effettuano il trattamento dei dati con strumenti elettronici, dovranno cautelarsi per evitare che le proprie credenziali di autenticazione possano essere conosciute da soggetti non autorizzati. Le conseguenze sono relative alla possibilità di accedere liberamente ai dati senza nessun controllo causando distruzioni, modifiche o acquisizioni non autorizzate. Tale tipologia di rischio è funzione del profilo di autenticazione associato all'operatore. Il livello del danno dipende, cioè, dal tipo di autorizzazione dell'operatore: scrittura, modifica, lettura, backup dei dati.

Gli operatori che trattano i dati sia con strumenti elettronici sia con strumenti non elettronici, possono causare dei danni ai dati per motivi di distrazione, inconsapevolezza, inesperienza dell'utilizzo dei dispositivi di accesso o errori materiali. Rientrano in tale categoria i seguenti eventi:

- Diffusione inconsapevole all'esterno dei supporti di memorizzazione e/o documenti contenenti i dati
- supporti di memorizzazione e/o documenti anche fotocopiati lasciati incustoditi
- supporti di memorizzazione e/o documenti contenenti i dati conservati all'interno degli appositi archivi e lasciati aperti senza custodia
- comunicazioni verbali dei dati fra operatori in presenza di personale esterno o non autorizzato
- comunicazioni scritte agli interessati (alunni, genitori o chi ne fa le veci) lasciate in contenitori aperti
- consegna di documenti e/o dati su supporti di memorizzazione a persona che dichiara falsa identità dell'interessato o falsa delega dello stesso

- allontanamento dal dispositivo di accesso senza interdizione della funzionalità mediante maschera di richiesta delle credenziali di accesso
- problemi tecnici non evidenziati.

Tutti gli operatori sono tenuti a rispettare le disposizioni del presente documento in riferimento al D.Lgs. 196/2003, con particolare attenzione ai danni causati da azioni fraudolente e sleali. Le conseguenze di tali azioni sono relative alla divulgazione e all'accesso dei dati che possono provocare distruzioni, modifiche o acquisizioni non autorizzate. Le ripercussioni sono anche relative alle sanzioni amministrative e penali come indicato ai seguenti articoli del D.Lgs. 196/2003:

- Art. 163 – violazioni di notificazione: "*Chiunque, essendovi tenuto,* [cioè il titolare] *non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica"*
- Art. 167 - trattamento illecito: *"Salvo che il fatto costituisca più grave reato, chiunque,* [cioè titolare responsabili e incaricati] *al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi…"*
- Art. 169 - Omessa adozione delle misure di sicurezza: perseguibile chiunque, essendovi tenuto, cioè titolare e responsabili e, alla luce del Disciplinare tecnico in materia di misure minime di sicurezza, Allegato B. -di cui agli art. da 33 a 36 del D.Lgs.196/2003-, anche gli incaricati
- Art. 170 – Inosservanza dei provvedimenti del Garante: "*Chiunque, essendovi tenuto,* [cioè titolare e responsabili] *non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni".*

Eventi che agiscono sugli apparati di automazione

Gli apparati di automazione riguardano ogni tipologia di gestione elettronica agente negli apparati informatici. In particolare dovranno essere controllati tutte le unità di accesso ai dati (PC) dell'amministrazione ed ogni possibile accesso in rete.

I programmi indesiderati come virus, cavalli di Troia, spyware si introducono nel sistema per mezzo di servizi Internet come e-mail e FTP oppure attraverso i driver (floppy e CD-ROM) di un sistema di accesso. La natura solitamente nociva di tali applicativi può provocare danni irreparabili oppure rendono possibili operazioni di accessi esterni indesiderati. Tali azioni sono causate da eventi non imputabili, in genere, agli operatori interni, a meno di azioni

fraudolente o sleali.

La ricezione di posta elettronica indesiderata (spamming) pur potendo creare aspetti di disagio durante le normali operazioni in rete, è da considerarsi, tuttavia, un evento non pericoloso per l'integrità dei dati.

Si ritiene rilevante la possibilità di guasti anche accidentali alle macchine, alle apparecchiature e ai componenti. Gli eventi possibili sono:

- Interruzione di link fisici di rete con conseguente indisponibilità dell'accesso ai database depositati nel server
- Interruzione o guasto degli apparati attivi della LAN con conseguente indisponibilità dell'accesso ai database
- Guasto ai PC contenenti dati oggetto di trattamento in particolare alle unità di massa (Hard disk) alle schede di rete, all'alimentatore, alle memorie centrali, al S.O., al software di gestione

Gli eventi relativi ai guasti possono provocare alterazione dei dati o perdite degli stessi.

I tentativi di attacco esterni sono finalizzati a bloccare o rallentare i sistemi oppure a catturare o distruggere i dati. Particolare attenzione si dovrà prestare ai seguenti tipi di attacchi:

- Attacchi di tipo DOS (Denial of Service): tendono a bloccare o rallentare il sistema informatico creando difficoltà ai soggetti di operare le normali funzioni di trattamento.
- IP spoofing: si tratta del tentativo di falsificare un indirizzo IP per favorire l'accesso al sistema che autorizza quel particolare indirizzo. In tal modo è possibile accedere liberamente ai dati.
- Sniffing: si tratta dell'ascolto in rete di possibili transiti di dati in modo da intercettarli e catturarli.

Eventi relativi al contesto fisico

Il rischio di accesso o di distruzione dei dati è particolarmente accentuato qualora siano presenti delle vulnerabilità nell'ambiente fisico in cui si svolge il trattamento dei dati.

L'accesso ai locali dell'amministrazione da parte di persone non autorizzate o esterne è da ritenersi un rischio di elevata entità soprattutto se restano incustoditi documenti, contenitori, armadi o terminali di accesso alla sottorete di amministrazione. Le intrusioni nei locali possono avvenire anche durante le ore di chiusura a seguito di azioni di scasso e furto dei dati contenuti in supporti elettronici e non. Fanno parte della stessa categoria di rischio azioni dolose e gli eventi accidentali distruttivi causati da agenti esterni come errori

umani, incendi e guasti alla rete elettrica che provocano danni soprattutto alle apparecchiature e alle macchine del sistema informatico.

La Tabella 5 riassume i rischi che incombono sui dati trattati con strumenti elettronici mentre nell'allegato 2 sono riportate le regole che gli incaricati dovranno rispettare ai fini della sicurezza dei dati personali.

Tabella 5 – Analisi dei rischi:

ANALISI DEI RISCHI			
Evento		Impatto sulla sicurezza dei dati	Riferimento misure d'azione
Comportamenti degli operatori	Furto di credenziali di autenticazione	accesso ai dati senza nessun controllo causando distruzioni, modifiche o acquisizioni non autorizzate	gestione delle credenziali, logging, IDS, gestione della rete
	Carenza di consapevolezza, disattenzione o incuria	modifica e perdita dei dati	backup
	Comportamenti sleali o fraudolenti	accesso ai dati senza nessun controllo causando distruzioni, modifiche o acquisizioni non autorizzate	gestione delle credenziali, logging, IDS, gestione della rete
	Errore materiale	accesso ai dati senza nessun controllo causando distruzioni, modifiche o acquisizioni non autorizzate	gestione delle credenziali, logging, IDS, gestione della rete
Eventi relativi agli strumenti	Azione di virus informatici o di codici malefici	danni ai database e accessi esterni indesiderati	antivirus, firewall, IDS, gestione della rete, logging, antivirus su PC
	Spamming o altre tecniche di disturbo senza sabotaggi	nessun danno	antivirus, firewall, IDS, gestione della rete, logging,antivirus su PC
	Malfunzionamento, indisponibilità o degrado degli strumenti	modifica e perdita dei dati	backup
	Accessi esterni non autorizzati	blocco o rallentamento dei sistemi, accesso non autorizzato o distruzione dei dati	firewall, IDS, gestione della rete, logging
Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	accesso ai dati senza nessun controllo causando distruzioni, modifiche o acquisizioni non autorizzate	gestione delle credenziali, logging, IDS, gestione della rete, gestione delle credenziali
	Asportazione e furto di strumenti contenenti dati	accesso ai dati senza nessun controllo causando distruzioni, modifiche o acquisizioni non autorizzate	gestione delle credenziali, logging, IDS, gestione della rete, gestione delle credenziali
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	modifica e perdita dei dati	backup

	Guasto ai sistemi complementari(impianto elettrico, climatizzazione)	modifica e perdita dei dati	backup
	Errori umani nella gestione della sicurezza fisica	modifica e perdita dei dati	backup

Misure di sicurezza esistenti o da realizzare

I rischi individuati nella sezione precedente vanno ulteriormente ridotti mediante l'introduzione di sistemi di sicurezza automatici ed idonee procedure di gestione della rete. Le misure da intraprendere o già intraprese per evitare o perlomeno ridurre i rischi sull'integrità dei dati, consistono in interventi tecnici o organizzativi e in attività di verifica e controllo periodici, necessari per assicurare nel tempo, la dovuta efficienza.

Le regole da adottare per evitare che le credenziali di autenticazione possono essere utilizzate da soggetti non autorizzati, consistono nell'adottare una valida gestione delle credenziali il cui incarico è affidato **al DSGA**. Tale gestione è valida se sono rispettate le seguenti regole:

- Le parole chiavi attive (nome utente e password) vanno conservate in luogo sicuro e affidate a ciascun incaricato mediante un documento in formato elettronico o cartaceo da conservare a cura del destinatario
- Almeno la password dovrà essere composta da minimo 8 caratteri, dovrà contenere caratteri vari e non potrà essere formata da parole di facile individuazione
- Se il sistema lo consente la parola chiave dovrà essere modificata dall'incaricato al primo utilizzo
- Le parole chiavi dovranno essere aggiornate almeno ogni tre mesi in quanto si tratta di dati sensibili, dopo tale periodo vanno disattivate e non più riutilizzate, salvo per motivi di manutenzione
- Le parole chiavi saranno disattivate in presenza di un accesso non autorizzato con la stessa parola chiave.
- In caso di prolungata assenza o impossibilità dell'incaricato a svolgere i propri compiti qualora si ritenga necessario la sostituzione con un altro soggetto, si dovrà assegnare a quest'ultimo una parola chiave temporanea valida solo per il periodo necessario. Tale regola vale anche in caso di supplenze, o assunzioni a tempo determinato. Dopo il periodo di utilizzo la parola chiave dovrà essere disattivata

Occorre svolgere operazioni di monitoraggio e logging periodici per mettere in risalto eventuali tentativi di violazione delle autorizzazioni. Tali operazioni possono essere realizzate mediante il server di controllo della LAN e mediante le funzioni del sistema di protezione centralizzato. La gestione della rete è a cura dell'amministratore di sistema il quale provvederà ad effettuare controlli IDS (Intrusion Detection Software) mediante i quali sono rilevati possibili

attività di attacco.

Tutti gli operatori devono svolgere le proprie mansioni prestando molta cura alle operazioni che svolgono per evitare rischi dovuti ad incurie o distrazioni. In particolare dovranno essere rispettate le seguenti regole generali:

- I dati contenuti in supporti di memorizzazione elettronici o in documenti cartacei non dovranno essere lasciati incustoditi neanche temporaneamente
- I dati contenuti in supporti di memorizzazione elettronici o in documenti dovranno essere sempre conservati all'interno degli appositi contenitori, armadi, cassettiere e casseforti controllando la corretta chiusura a chiave negli orari di chiusura o comunque in assenza anche temporanea degli incaricati
- Le comunicazioni verbali o qualunque altra comunicazione che utilizzano tecnologie elettroniche come telefono interno, fax, fotocopie che avessero come ARGOmento la divulgazione di dati personali e sensibili non devono essere effettuate in presenza di personale esterno o non autorizzato
- Le comunicazioni scritte dovranno essere conservate in contenitori chiusi
- È necessario accertare l'identità dell'interessato o di chi ne fa le veci (alunni maggiorenni o genitori) prima di comunicare o consegnare i dati di suo interesse.

- Interdire le funzionalità dei dispositivi durante i periodi di assenza, pausa o allentamento momentaneo, utilizzando anche tecniche automatiche di disattivazione del sistema impostando, in questo caso, la disattivazione dopo massimo cinque minuti di inattività.
- Effettuare copie di backup almeno una volta al mese mediante supporti di memorizzazione removibile e conservare in contenitori con serratura. Tale supporto andrà installato almeno sul server di amministrazione. Le copie di backup possono essere sovrascritte sullo stesso supporto cancellando definitivamente quello precedente. In caso di ripristino dei dati, riutilizzare l'ultima copia di backup effettuata. L'esecuzione del backup può essere impostata con procedure automatiche direttamente sul sistema centralizzato. Responsabile per il controllo e la gestione delle funzioni di backup è l'amministratore di sistema.

La protezione dei dati da programmi dannosi come virus, cavalli di Troia, spyware deve essere controllata da sistemi di protezione idonei, le cui funzionalità sono state descritte nella sezione 8.1. Si rende necessario, tuttavia, aggiornare almeno con cadenza settimanale gli antivirus su ciascuna macchina contenenti archivi elettronici descritti nell'allegato1 (anche quelle che non gestiscono accessi al sistema ARGO-SIDI) in modo da prevenire possibili infezioni dai driver di sistema (floppy, CD ROM, ecc.).

Si rende necessario, inoltre, una manutenzione ordinaria dell'intera rete e del sistema centrale di sicurezza informatico utilizzando tecniche di testing o

controlli manuali degli apparati in modo da garantire un alto livello di efficacia del sistema informatico e ridurre il rischio di guasti accidentali. Tale manutenzione dovrà essere effettuata almeno una volta ogni tre mesi a partire dalla data del presente documento. Si dovrà controllare in particolare:

- Il sistema di backup mediante test
- Log sul S.O. del sistema centrale di amministrazione
- Controllo delle memorie fisiche del sistema centrale (Hard disk)
- Controllo del RDBMS
- Controllo visivo del cablaggio (canaline, cavi di connessione, concentratori)
- Test di connessione da ciascun sistema di accesso client
- Verifica di software installato non autorizzato e dannoso su tutte le macchine della sottorete di amministrazione
- Gruppi di continuità (UPS) del sistema centrale mediante test
- Log del sistema di protezione centrale

Responsabile della manutenzione ordinaria è l'amministratore di sistema.

Il controllo degli accessi esterni e non autorizzati è una misura che va adottata sia sui sistemi di gestione elettronica sia sui contenitori dei documenti e nei locali dove essi sono custoditi.

Per quanto riguarda il controllo di accessi non autorizzati al sistema informativo, occorre prestare attenzione alle situazioni che potrebbero rilevarsi come possibili occasioni di accesso incontrollato (ad esempio sniffing interno alla LAN). In particolare:

- Gli armadi del cablaggio devono restare chiusi. Le chiavi saranno custodite dall'amministratore del sistema che le conserverà in apposito cassetto
- L'uso delle cartelle condivise nei PC della sottorete di amministrazione dovrà essere evitato, se si rende necessario il loro utilizzo occorre proteggerle con password utilizzando le regole viste all'inizio della presente sezione
- Evitare di impiegare indirizzi IP pubblici per le macchine della sottorete di amministrazione. In base alle esigenze, su autorizzazione del titolare, impostare le politiche di accesso al firewall riducendo le eventuali porte TCP in ingresso

Occorre svolgere operazioni di monitoraggio e logging periodici per mettere in risalto eventuali tentativi di violazione degli accessi. Tali operazioni possono essere realizzate mediante il server di controllo della LAN e mediante le funzioni del sistema di protezione centralizzato. La gestione della rete è a cura dell'amministratore di sistema il quale effettuerà controlli IDS per rilevare possibili attività di attacchi.

I cassetti, gli armadi blindati e la cassaforte dovranno essere controllati periodicamente (almeno una volta l'anno) con particolare riferimento

all'efficienza e alla sicurezza delle serrature e delle chiavi. Una prima verifica dovrà effettuarsi a partire dalla data di rilascio del presente documento. I locali in cui sono ubicati gli archivi dovranno essere dotati di porte dotate di serratura efficiente. A tal proposito si rende necessario il controllo delle serrature di tutte le porte dei locali amministrativi e provvedere alla riparazione in caso di evidenti guasti. È necessario sempre evidenziare i locali vietati al pubblico e i locali accessibili al pubblico con l'indicazione degli orari di apertura e chiusura. Potranno accedere agli archivi e custodire le chiavi degli archivi e delle porte dei locali: il Dirigente Scolastico, il Direttore Amministrativo, gli incaricati dell'amministrazione.

Per i sistemi antincendio e di allarme si dovrà effettuare una manutenzione ordinaria almeno annuale, controllando l'efficienza dei sensori e delle centraline di comando.

L'affidamento a persone fisiche o giuridiche esterne all' **Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG)** che per particolari mansioni o incarichi effettuano il trattamento dei dati, il titolare o il responsabile nominerà la persona esterna con atto scritto in cui sono indicate le norme di comportamento previste.

In caso di adeguamento delle misure minime da parte di soggetti esterni l'installatore consegna al titolare una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni previste disciplinare tecnico del D.Lgs. 196/2003 allegato B.

La Tabella 6 riassume le misure minime di sicurezza già adottate o da adottare, mentre la Tabella 7 riporta le schede descrittive per ciascuna misura adottata.

Tabella 6 – Misure di sicurezza adottate:

Tabella 6 : MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE								
Misura	Rischio contrastato	Trattamento interessato	Eventuale banca dati interessata	Riferimento scheda analitica	Misura già in essere	Misura da adottare	Data prevista misura da adottare	Periodicità e responsabilità dei controlli
gestione credenziali mediante regole di creazione delle password	accesso ai dati senza nessun controllo	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	1	SI	\	\	3 mesi amministratore di sistema
riduzione dei rischi dovuti ad incurie	modifica e perdita dei dati	tutti	\	2	SI	\	\	tutti gli operatori
antivirus su ciascuna macchina di amministrazione	danni ai database e accessi esterni indesiderati	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	3	SI	\	\	settimanale tutti gli operatori
manutenzione PC	blocco o rallentamento dei sistemi, accesso non autorizzato o distruzione dei dati	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	4	SI	\	\	trimestrale amministratore di sistema, soggetti esterni

Tabella 6 : MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

Misura	Rischio contrastato	Trattamento interessato	Eventuale banca dati interessata	Riferimento scheda analitica	Misura già in essere	Misura da adottare	Data prevista misura da adottare	Periodicità e responsabilità dei controlli
backup dei dati ARGO-SIDI sul server di amministrazione e backup dei documenti elettronici	modifica e perdita dei dati	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	5	SI	\	\	settimanale tutti gli operatori
suddivisione della LAN nelle sottoreti didattica e amministrazione	accesso ai dati non autorizzati all'interno della LAN	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	6	SI	\	\	mensile amministratore di sistema
negazione dell'accesso verso la sottorete amministrazione da parte degli utenti della didattica, ad eccezione del server della didattica	accesso ai dati non autorizzati all'interno della LAN	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	7	SI	\	\	mensile amministratore di sistema
Intrusion Detection System (IDS)	accesso ai dati dall'interno	dati e documenti trattati con strumenti	SISSI-SIDI	8	SI	\	\	3 mesi amministratore di sistema

Tabella 6 : MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

Misura	Rischio contrastato	Trattamento interessato	Eventuale banca dati interessata	Riferimento scheda analitica	Misura già in essere	Misura da adottare	Data prevista misura da adottare	Periodicità e responsabilità dei controlli
		elettronici						
antivirus e filtraggio e-mail	danni ai database e accessi esterni indesiderati	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	9	SI	\	\	mensile amministratore di sistema
filtraggio accessi Internet	danni ai database e accessi interni/esterni indesiderati	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	10	SI	\	\	trimestrale amministratore di sistema, soggetti esterni
raggruppamento dei tipi di utenti con controllo degli accessi	danni ai database e accessi interni/esterni indesiderati	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	11	SI	\	\	
blocco di tutte le porte TCP verso la sottorete di amministrazione	danni ai database e accessi interni/esterni indesiderati	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	12	SI	\	\	

Tabella 6 : MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

Misura	Rischio contrastato	Trattamento interessato	Eventuale banca dati interessata	Riferimento scheda analitica	Misura già in essere	Misura da adottare	Data prevista misura da adottare	Periodicità e responsabilità dei controlli
antivirus su ciascuna macchina di amministrazione	danni ai database e accessi esterni indesiderati	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	13	SI	\	\	
manutenzione sistema informatico	blocco o rallentamento dei sistemi, accesso non autorizzato o distruzione dei dati	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	14	SI	\	\	
controllo di accessi non autorizzati al sistema informativo	accesso ai dati dall'esterno	dati e documenti trattati con strumenti elettronici	SISSI-SIDI	15	SI	\	\	
controllo periodico degli archivi fisici e dei locali	modifica e perdita dei dati	documenti trattati con strumenti non elettronici	\	16	SI	\	\	

Tabella 6 : MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE								
Misura	Rischio contrastato	Trattamento interessato	Eventuale banca dati interessata	Riferimento scheda analitica	Misura già in essere	Misura da adottare	Data prevista misura da adottare	Periodicità e responsabilità dei controlli
impianto antincendio	distruzione dei dati	tutti	\	17	SI	\	\	
impianto allarme	distruzione dei dati	tutti	\	18	SI	\	\	
protezione da guasti degli impianto elettrico: UPS al server di amministrazione	distruzione dei dati	documenti trattati con strumenti non elettronici	SISSI-SIDI	19	SI	\	\	
~~Impianto videosorveglianza~~	~~Intrusioni fisiche~~	~~tutti~~	~~\~~	~~20~~	~~NO~~	~~\~~	~~\~~	~~annuale titolare, responsabile~~

Tabella 7 – Scheda descrittiva delle misure adottate:

Tabella 7: SCHEDA DESCRITTIVA DELLE MISURE ADOTTATE			
Scheda nr.	Misura	Descrizione sintetica	Elementi descrittivi

Tabella 7: SCHEDA DESCRITTIVA DELLE MISURE ADOTTATE			
Scheda nr.	Misura	Descrizione sintetica	Elementi descrittivi
1	gestione credenziali mediante regole di creazione delle password	generazione di nome utente e password per ciascun incaricato, le regole da rispettare sono quelle descritte nel DPS	Impiego delle funzioni di accesso mediante password intrinseche dei S.O. delle macchine
2	riduzione dei rischi dovuti ad incurie	conservazione e custodia dei dati trattati con mezzi elettronici e non	Rispetto delle regole relative alla divulgazione dei dati come descritto dettagliatamente nel DPS, sia utilizzando mezzi elettronici sia mediante documenti cartacei
3	antivirus su ciascuna macchina di amministrazione	Protezione da accessi sulla macchina mediante supporti di memorizzazione (floppy, CDROM)	Gestione e controllo antivirus su ciascuna macchina della LAN di amministrazione
4	manutenzione PC	manutenzione ordinaria dei PC	Vanno applicati test utili per il controllo dell'efficienza del sistema informatico e del livello di sicurezza, le regole minime sono dettagliate nel DPS
5	backup dei dati ARGO-SIDI sul server di amministrazione	Impiego di supporti fisici di backup	Il backup realizzato secondo le regole descritte nella sezione 10.1
6	suddivisione della LAN nelle sottoreti didattica e amministrazione	sezionamento fisico e logico della LAN in 2 sottoreti: amministrazione e didattica.	armadio rackle 2 sottoreti possono essere gestite a livello centralizzato adottando politiche di

Tabella 7: SCHEDA DESCRITTIVA DELLE MISURE ADOTTATE			
Scheda nr.	Misura	Descrizione sintetica	Elementi descrittivi
			controllo e funzioni di firewall, filtraggio pacchetti, filtraggio applicativi (WEB. E-mail, ecc)
7	~~negazione dell'accesso verso la sottorete amministrazione da parte degli utenti della didattica, ad eccezione del server della didattica~~	~~realizzazione di un canale di accesso~~	~~creazione di un canale di accesso dalla sottorete di didattica alla sottorete di amministrazione per controlli e monitoraggio della rete~~
8	Intrusion Detection System (IDS)	abilitazione della funzione Intrusion Detection System (IDS) sul sistema di protezione centralizzato	Abilitazione della funzione Intrusion Detection System (IDS) con la quale sono rilevati possibili attività di attacchi esterni noti, compreso attacchi di tipo DOS (Denial Of Service)
9	antivirus e filtraggio e-mail	abilitazione della funzione antivirus e filtraggio e-mail sul sistema centralizzato per tutte le utenze	funzione antivirus centralizzato e filtraggio e-mail su tutte le postazioni della LAN con aggiornamento dei profili di utenza
10	filtraggio accessi Internet	abilitazione della funzione di filtraggio degli accessi Internet sul sistema di protezione centralizzato da parte degli utenti ritenuti non affidabili (alunni, personale esterno)	negazione degli accessi a siti non affidabili, blocco delle attività di download e degli applicativi ritenuti dannosi (IRC, chat, ecc.)
11	raggruppamento dei tipi di utenti con controllo degli accessi	suddivisione delle utenze in gruppi omogenei, e controllo centralizzato degli accessi e delle politiche di	suddivisione in utenze della rete di amministrazione, utenti per l'amministrazione di sistema,

Tabella 7: SCHEDA DESCRITTIVA DELLE MISURE ADOTTATE			
Scheda nr.	Misura	Descrizione sintetica	Elementi descrittivi
		protezione	alunni in laboratorio, docenti
12	blocco di tutte le porte TCP verso la sottorete di amministrazione	blocco a livello di firewall delle porte di accesso alla sottorete di amministrazione	blocco di accesso dall'esterno alle porte TCP
13	antivirus su ciascuna macchina di amministrazione	Protezione da accessi sulla macchina mediante supporti di memorizzazione (floppy, CDROM)	Gestione e controllo antivirus su ciascuna macchina della LAN di amministrazione
14	manutenzione sistema informatico	manutenzione ordinaria del sistema informatico	vanno applicate ogni test utile per il controllo dell'efficienza del sistema informatica e del livello di sicurezza, le regole minime sono dettagliate nel DPS
15	controllo di accessi non autorizzati al sistema informativo	adozione di politiche sul firewall	blocco delle porte TCP e configurazione NAT di tutte le postazioni della LAN, ad eccezione di macchine della sottorete didattica
16	controllo periodico degli archivi fisici e dei locali	controllo e manutenzione delle porte di accesso e delle serrature degli archivi	sostituire le parti difettose
17	impianto antincendio	manutenzione ordinaria dell'impianto antincendio	controllo sensori e centralina di controllo
18	impianto allarme	manutenzione ordinaria dell'impianto di allarme	controllo sensori e centralina di controllo

Tabella 7: SCHEDA DESCRITTIVA DELLE MISURE ADOTTATE			
Scheda nr.	Misura	Descrizione sintetica	Elementi descrittivi
19	protezione da guasti degli impianto elettrico: UPS al server di amministrazione	manutenzione UPS	Controllo della funzionalità dell'UPS sul sistema centrale mediante test
20	~~Impianto videosorveglianza~~	~~manutenzione ordinaria dell'impianto di videosorveglianza~~	~~Controllo telecamere e monitor~~

Criteri e modalità per il ripristino della disponibilità dei dati

Gli eventi che implicano la perdita dei dati e la conseguente sospensione dei servizi di trattamento, sono affrontati mediante procedure verso cui gli incaricati devono attenersi, utilizzando opportuni strumenti tecnologici atti al ripristino dei dati stessi.

I dati sottoposti alle procedure di ripristino in caso di danni causati dai rischi elencati nella Tabella **5** – Analisi dei rischi:

sono quelli contenuti negli archivi elettronici indicati negli allegati 1 e 2. Tali archivi fanno parte di uno delle seguenti categorie di dati:

- **Documenti elettronici redatti con software Office presenti negli elaboratori EL00, EL01, EL02, EL03, EL04, EL05, EL06, EL07;**
- **Dati contenuti nei documenti di posta elettronica degli elaboratori EL01, EL02, EL03, EL04, EL05, EL06, EL07;**
- **Dati del software ministeriale ARGO-SIDI contenuti nel server EL00.**

Il punto 18 dell'allegato B del D.Lgs. 196/03 prevede il salvataggio dei dati periodico con cadenza settimanale. Tale procedura si concretizza nell'impiego di tecniche di backup dei dati appartenenti alle categorie su elencate.

L'allegato B del D.Lgs. 196/03 indica le modalità di adozione di "misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni". Tale procedura si concretizza adottando criteri e metodi atti alla protezione ed al ripristino del funzionamento degli strumenti elettronici con le modalità di seguito descritte.

Tecniche di backup

- ***Documenti elettronici redatti con software Office***: I documenti elettronici redatti con software Microsoft Office (word, excel, power point, ecc.) contenenti dati personali da sottoporre ai criteri di ripristino, devono essere memorizzati in apposita cartella dell'elaboratore. Poiché non sono previsti misure di sicurezza informatica avanzata, tale cartella non deve essere lasciata condivisa salvo nei casi in cui si necessita inviare un documento ad un altro elaboratore nei casi di lavoro di gruppo. In tal caso è possibile condividere la cartella solo per il tempo strettamente necessario per l'operazione di trasferimento. In alternativa è possibile utilizzare tecniche avanzate come:

- Server di dominio dove sono memorizzati tutti i documenti elettronici in apposita cartella. L'accesso è consentito solo ai client che avranno un parola

chiave. I client possono essere suddivisi in categorie dove ciascuno potrà avere la propria area personale, mentre altri potranno accedere solo per lettura oppure non avere l'autorizzazione ad accedere.

- Impiego di un sistema di backup automatico su supporto removibile a nastro magnetico montato sul server di dominio. Il backup sarà impostato per salvare i dati settimanalmente
- Impiego di software e sistemi operativi recenti che includono strumenti di protezione quali backup automatici e crittografia dei documenti e delle cartelle.

Allo stato attuale il backup dei dati dei documenti elettronici dovrà essere effettuato manualmente o utilizzando gli strumenti automatici del sistema operativo se questo lo permette. Tale procedura deve essere effettuata settimanalmente, mentre i supporti di memorizzazione devono essere consegnati al DSGA e conservati in cassaforte. È opportuno impiegare due supporti di memorizzazione alternativamente (uno per ogni settimana) in modo da tenere comunque una copia meno recente, ma sicuramente funzionante, ciò per porre rimedio al fallimento o al danno dell'ultima operazione di backup. In caso di ripristino dei dati riutilizzare l'ultima copia di backup effettuata. Responsabile per il controllo e la funzionalità del sistema di backup è l'amministratore di sistema

- ***Dati contenuti nei documenti di posta elettronica.*** La posta elettronica è memorizzata in una cartella standard impostata dal programma di posta elettronica (normalmente Outlook Express). Qualora si rendesse necessario le copie di backup seguono le stesse regole indicate a proposito dei documenti elettronici redatti con software Office.
- ***Dati del software ARGO-SIDI***. ARGO-SIDI è un software clien-server basato su ODBC centralizzato. Pertanto tutti i dati sono conservati nel server utilizzando le tecniche di protezione del database relazionale Sybase. Le tecniche di backup di ARGO-SIDI prevedono la possibilità di salvare dati contenuti nelle varie aree (alunni, bilancio, ecc.) impostando opportunamente il periodo di salvataggio. Tale procedura deve essere effettuata settimanalmente, mentre i supporti di memorizzazione devono essere consegnati al **DSGA** e conservati in cassaforte. È opportuno impiegare due supporti di memorizzazione alternativamente (uno per ogni settimana) in modo da tenere comunque una copia meno recente, ma sicuramente funzionante, ciò per porre rimedio al fallimento o al danno dell'ultima operazione di backup. In caso di ripristino dei dati riutilizzare l'ultima copia di backup effettuata. Responsabile per il controllo e la funzionalità del sistema di backup è l'amministratore di sistema. Si consiglia di adottare un sistema di backup automatico su supporto removibile a nastro magnetico montato sul server.

Tecniche di ripristino del funzionamento degli strumenti elettronici

Si rende necessario una manutenzione ordinaria della rete utilizzando tecniche di testing o controlli manuali degli apparati in modo da garantire un alto livello di efficacia del sistema informatico e ridurre il rischio di guasti accidentali. Tale manutenzione dovrà essere effettuata almeno una volta ogni tre mesi a partire dalla data del presente documento. Intendendo per PC le macchine con le quali si elaborano dati oggetto del presente documento (sono esclusi pertanto macchine impiegati per scopi diversi, come PC di laboratorio, PC per la didattica, ecc.), si dovrà controllare in particolare:

- Test sul S.O. dei PC
- Controllo delle memorie fisiche dei PC (Hard disk)
- Controllo visivo della LAN1 (sottorete amministrazione) e controllo delle relative politiche di protezione adottate nel sistema di protezione centralizzato.
- Verifica di software gestionale e di Office automatico (Microsoft Office) installato
- Verifica di software installato non autorizzato e dannoso su tutti i PC e le macchine della LAN1 (sottorete di amministrazione)
- Verifica delle intrusioni utilizzando informazioni log ed eventuale azioni correttive
- Verifica delle funzionalità del server ARGO-SIDI sia sui client sia sul server
- Gruppi di continuità (UPS) dei PC
- Verifica e simulazione delle tecniche di backup

Responsabile della manutenzione ordinaria è l'amministratore di sistema.

Interventi formativi

Il titolare del trattamento a partire dalla data del presente documento approntera un corso di formazione rivolto a tutti gli operatori con l'obiettivo di rendere praticabili le misure di sicurezza e le regole di attuazione nel contesto relativo all' **Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG)**.

Qualora si rendesse necessario saranno svolti corsi di aggiornamento all'inizio di ogni anno scolastico. Ciò anche in relazione a novità che si dovessero presentare nelle norme di legge e/o in relazione all'evoluzione tecnica del settore.

Le attività formative saranno opportunamente verbalizzate.

San Severo (FG), ___/___/_____

Il Titolare _____

Allegato 1: descrizione dettagliata del trattamento dei dati personali

T1 – Alunni. Dati personali trattati da docenti e dal Dirigente Scolastico

Tipologia di dati:

- dati comuni di alunni per qualsiasi attività didattica e organizzativa
- dati sensibili di alunni relativi alla attività didattica per la scelta dell'insegnamento della religione
- dati sensibili di alunni per la registrazione di assenze per motivi di salute con certificati medici di avvenuta guarigione, giustificazioni di assenze per festività religiose
- dati sensibili di alunni di certificati medici per esonero da educazione fisica
- dati comuni di alunni di comunicazioni scritte scuola-famiglia (libretto personale)
- dati sensibili di alunni portatori di handicap e relative documentazioni del proprio stato
- dati particolari di alunni per note disciplinari su registri
- dati particolari di alunni per valutazioni, votazioni, profitto, condotta, profilo psicologico e attitudinale, ecc. riportati su registri
- dati particolari di alunni relativi agli elaborati scritti come temi riportanti informazioni sulla propria sfera personale e familiare
- dati sensibili di alunni relativi a conoscenze casuali durante le attività o comunicate dai genitori, come problemi di salute, situazioni familiari particolari relativi a uno o più membri della famiglia
- dati comuni di alunni dei registri di classe e dei registri dei docenti
- dati comuni di alunni del registro dei verbali dei Consigli di classe
- dati comuni di alunni dei registri e documenti di esami e concorsi
- dati comuni di alunni per attività varie della scuola
- dati comuni di alunni in caso di visite d'istruzione o viaggi
- dati comuni delle elezioni degli organi collegiali
- dati sensibili di attività del sindacato interno
- dati comuni del POF (Piano Offerta Formativa)
- dati comuni dell'orientamento scolastico

Modalità di trattamento

- I registri sono custoditi dagli incaricati e conservati in luogo chiuso
- I certificati medici di qualunque natura dopo una consultazione per motivi didattici vanno consegnati alla segreteria
- Gli elaborati degli studenti sono di norma custoditi in archivio sicuro. Nel caso essi contengono dati sensibili, vengono consegnati in busta chiusa alla segreteria per una conservazione a parte
- Le informazioni personali degli alunni vanno tenuti con riserbo. Se esiste qualche comunicazione scritta va conservata in luogo sicuro a cura della segreteria
- I registri vengono raccolti da un collaboratore scolastico e conservati in luogo sicuro. La consegna è effettuata da un collaboratore scolastico all'inizio delle lezioni

- I registri sono conservati nell'armadietto del docente e chiuso a chiave

Archivi non elettronici

- Archivio corrente alunni (contiene Fascicoli Personali)
- Archivio registri e prospetti
- Archivio degli elaborati dell'anno corrente

Archivi elettronici : Nessuno
Elenco dati trattati con strumenti elettronici: Nessuno
Elenco dati comunicati a strutture esterne:

- Dati comuni forniti a strutture in occasione di visite e viaggi

Categoria di trattamenti operati (indicati nella Tabella 4 **– Strutture preposte al trattamento:**

Descrizione	*ID Trattamento*	*n. progressivo*	*Tipo trattamento (1)*	*Tipo dato (2)*
didattica e attività correlate	T1	1	C	CS
Handicap, stato di salute	T1	2	C	CS

(1) *C: cartaceo*

E: elettronico

(2) *C: dati comuni*

S: dati sensibili

G: dati giudiziari

T2 – Alunni. Dati personali trattati Assistenti Amministrativi, D.S.G.A e Dirigente Scolastico:

Tipologia di dati:

- dati comuni di alunni per iscrizione annuale
- dati comuni di alunni per documentazione scolastica riguardante il loro rendimento come pagelle, valutazioni
- dati sensibili di alunni per la scelta dell'insegnamento della religione e relativa valutazione
- dati comuni di alunni per la gestione delle tasse e contributi scolastici
- dati sensibili di alunni per documenti riguardanti lo stato patrimoniale, dichiarazioni fiscali, situazione familiari al fine di ottenere esoneri da tasse, contributi e benefici economici
- dati comuni di alunni e loro familiari per attività varie della scuola e per l'elezione degli Organi Collegiali
- dati sensibili di alunni stranieri immigrati riguardante le generalità, l'origine etnica, la religione ecc.
- dati sensibili di alunni riguardanti particolari situazioni riferite allo stato di salute contenuti in documenti, certificati medici o comunicazioni da parte della famiglia
- dati sensibili (in alcuni casi anche giudiziari) di alunni relativi a documenti che attestano quale è la persona esercente la patria potestà per alunni minorenni in situazione particolare o in stato di affido
- dati sensibili di alunni relativi a documenti e certificati sullo stato di handicap che incidono sulla didattica (dato sensibile in quanto idoneo a rivelare lo stato di salute)
- dati sensibili di alunni relativi a test psicologici o psicoattitudinali
- dati comuni di alunni contenuti in certificati prodotti dalla scuola stessa quali iscrizione, frequenza, profitto, carriera scolastica, ecc.

- dati comuni di alunni relativi a documenti prodotti da altri enti quali iscrizione, frequenza, profitto, carriera scolastica, ecc.
- dati sensibili di alunni per assenze dovuti a motivi quali salute e relativi certificati medici, famiglia, festività religiose anche non cattoliche
- dati sensibili di alunni di certificati medici per esonero da educazione fisica
- dati sensibili di alunni relativi a provvedimenti disciplinari gravi (sospensione, espulsione, ecc.)
- dati comuni e sensibili di alunni relativi a valutazioni intermedie e finali, votazioni, profitto, grado di impegno, condotta, profilo psicologico e attitudinale, ecc.
- dati comuni e sensibili di alunni per certificazioni mediche a seguito di infortuni a scuola per denuncia a Questura, Inail, assicurazione della scuola
- dati comuni di alunni relativi a pagelle, diplomi, prospetti degli esiti e delle ammissioni agli esami, registro dei voti e delle assenze, registro degli esami di maturità e di idoneità o integrativi
- dati comuni e sensibili contenuti in lettere trasmesse alla famiglia su profitto, provvedimenti disciplinari, comportamenti inadeguati, assenze ingiustificate ecc.
- dati comuni e sensibili contenuti in lettere trasmessi o documenti trasmessi dagli alunni o dalla famiglie che segnalino comportamenti (professionali e non) inadeguati o censurabili di docenti, personale o altri alunni, ivi comprese petizioni e richieste di ispezioni da parte delle Autorità scolastiche superiori
- dati comuni e sensibili relativi all'orientamento scolastico in ingresso e in uscita riguardanti anche profili psicologici
- dati comuni di alunni riguardanti prestiti della biblioteca
- dati comuni di alunni riguardanti la partecipazione di alunni a tirocini formativi/stages
- dati comuni di alunni riguardanti l'organizzazione di viaggi con agenzie di viaggio
- dati comuni di alunni relativi alla organizzazione di classi e del relativo organico
- dati giudiziari di alunni relativi ad eventuali denuncie o atti per violazioni civili e penali,
- dati sensibili e a volte giudiziari relativi ad atti riguardanti l'obbligo scolastico e intervento dell'autorità per inosservanza dell'obbligo scolastico

Modalità di trattamento

- Tutti i fascicoli relativi agli alunni al termine della carriera scolastica o in caso di ritiro, sono depositati in storico
- I dati di alunni possono essere trasmessi ad altri enti come previsto dall'art. 18 comma 4 anche per vie telematiche come alle misure minime di sicurezza descritte in questo documento e in conformità all'allegato B parte A del D.LGS. 196/03
- I dati comuni e sensibili di alunni sono trattati con strumenti elettronici, caratterizzati da funzioni come indicato nelle misure minime di sicurezza descritte in questo documento e in conformità all'allegato B parte A del D.LGS. 196/03
- La gestione dei registri dei voti e delle assenze e del Registro degli esami di maturità sono trattati con strumenti cartacei e strumenti elettronici, caratterizzati da funzioni come indicato nelle misure minime di sicurezza descritte in questo documento e in conformità all'allegato B parte A del D.LGS. 196/03
- **La trasmissione con strumenti cartacei o elettronici di dati di alunni riguardanti il curriculum o altri dati riguardanti la sfera personale, ad organizzazioni esterne (aziende, enti, ecc.), avviene solo su consenso dell'interessato o di chi ne fa le veci**
- I fascicoli di alunni sono conservati in archivi non elettronici all'interno degli uffici preposti come indicato nella sezione relativa all'elenco degli archivi
- I dati prodotti con strumenti elettronici sono conservati in archivi elettronici come indicato nella sezione relativa all'elenco degli archivi e trasmessi all'occorrenza per via telematica agli archivi remoti del Ministero dell'Istruzione
- Gli atti relativi alla produzione di certificati o documenti sono prodotti con strumenti elettronici quali software Microsoft Office (Word, Excel, ecc.) e depositati in archivi elettronici e cartacei come indicato nella sezione relativa all'elenco degli archivi

Archivi non elettronici

- Archivio corrente alunni (contiene Fascicoli Personali)
- Archivio storico alunni (contiene Fascicoli Personali)
- Archivio registri e prospetti
- Archivio Diplomi
- Archivio di corrispondenza generale (esclusa le corrispondenza con singoli che dispongano di Fascicolo Personale)
- Archivio degli elaborati dell'anno corrente
- Archivio storico degli elaborati
- Archivio delle prove d'esame anno corrente

- Archivio storico delle prove d'esame

- ***Archivi elettronici*** :

  - Archivio ARGO-SIDI alunni
  - Archivio documenti elettronici 1 redatti con sw M.Office 1

- ***Elenco dati trattati con strumenti elettronici***:

  - Gestione Anagrafica alunni mediante area ARGO-SIDI alunni
  - Gestione votazioni analitiche nel corso dell'anno scolastico e finali mediante ARGO-SIDI alunni
  - Gestione votazioni analitiche nel corso dell'anno scolastico e finali mediante ARGO-SIDI alunni
  - Documenti generici redatti con programma di Office Automation (Microsoft Office)
  - Elenchi anagrafici contenenti dati comuni prodotti con documenti elettronici redatti mediante sw Office, trasmessi per via telematica, per posta elettronica o memorizzati su supporti di memorizzazione elettronici, trasmessi ad enti esterni quali ASL, enti pubblici, aziende e privati in occasione di visite guidate, viaggi e simili.
  - Gestione documenti elettronici redatti mediante sw Office, trasmessi per via telematica, per posta elettronica o memorizzati su supporti di memorizzazione elettronici, trasmessi ad enti di riferimento quali Inail, Questura, ASL per denuncia infortuni e casi di provvedimenti disciplinari

- ***Elenco dati comunicati a strutture esterne***:

  - Dati trasmessi ad altra scuola per trasferimento riguardante Fascicolo Personale (documenti anagrafici, documenti scolastici, ecc. o dati sensibili riguardanti lo stato di salute soltanto su consenso dell'interessato.
  - Elenchi anagrafici contenenti dati comuni prodotti con documenti elettronici redatti mediante sw Office, trasmessi per via telematica, per posta elettronica o memorizzati su supporti di memorizzazione elettronici, trasmessi ad enti esterni quali ASL, enti pubblici, aziende e privati in occasione di visite guidate, viaggi e simili
  - Documenti elettronici redatti mediante sw Office, trasmessi per via telematica, per posta elettronica o memorizzati su supporti di memorizzazione elettronici, trasmessi ad enti di riferimento quali Inail, Questura, ASL per denuncia infortuni e casi di provvedimenti disciplinari
  - Trasmissione ad enti pubblici di particolari pratiche, su richiesta dell'interessato, per ottenere determinati benefici.
  - Pubblicazione di documenti cartacei all'albo di prospetti con esiti scolastici intermedi, finali, di ammissione a esami, di risultato degli esami., nonché di elenchi di ammessi all'Istituto o ad altre iniziative.
  - Trasmissione con strumenti cartacei o elettronici di dati di alunni riguardanti il curriculum o altri dati riguardanti la sfera personale, ad organizzazioni esterne (aziende, enti, ecc.), previo consenso dell'interessato o di chi ne fa le veci

Categoria di trattamenti operati (indicati nella Tabella 4 **– Strutture preposte al trattamento:**

Descrizione	*ID Trattamento*	*n. progressivo*	*Tipo trattamento (1)*	*Tipo dato (2)*
attività amministrativa e altre attività correlate	T2	1	CE	CS
attività inerenti la didattica	T2	2	CE	CS
attività integrative	T2	3	CE	CS
stato di salute, handicap e psico attitudinali	T2	4	CE	CS
origine etnica e religiosa	T2	5	CE	CS
stati personali e familiari riservati	T2	6	CE	CSG
assicurazione, infortuni, denuncie, compresa eventuale applicazione D.Lgs 81/08	T2	7	CE	CSG

(1) *C: cartaceo*

E: elettronico

(2) *C: dati comuni*

S: dati sensibili

G: dati giudiziari

T3 - Personale dipendente. Dati personali trattati da Assistenti Amministrativi, DSGA e dal Dirigente Scolastico:

Tipologia di dati:

- Dati comuni e sensibili contenuti nei fascicoli del personale contenenti documenti riferibili alla persona e documenti prodotti da altri enti.
- Dati riservati sensibili e giudiziari riguardanti lo stato di salute o provvedimenti civili e penali contenuti in fascicoli appositi

- Dati comuni trasmessi ad altre scuole o da altre scuole di assunzione in servizio, di assenze , di particolari concessioni e di altri atti nel caso di docenti utilizzati a scavalco da più scuole; di orario scolastico, di impegni per riunioni, ecc., di partecipazione ad esami ed altri attività
- Dati comuni di dipendenti per attività varie della scuola

Assenze, permessi, congedi, aspettative e simili

- Dati sensibili riguardanti certificati medici generici per assenze per malattia
- Dati sensibili per registrazione delle assenze per malattia e relativi atti concessivi
- Dati sensibili per richieste, certificazioni, dichiarazioni e concessioni di permessi per handicap di un familiare, fruizione di permessi, riduzioni d'orario e simili per motivi di salute o per condizione di handicap o invalidità, aspettativa per motivi di salute (dato sensibile), assenze retribuite al 100% perché connesse a ricoveri ospedalieri, gravi patologie o dovute a terapie invalidanti certificate (art. 17 CCNL 2007) (dato sensibile) e relativi atti concessivi, permessi retribuiti o congedi per gravi e documentati motivi e per particolari patologie dei familiari come definiti dall'art. 433 C.C. e relativi atti concessivi, permesso per particolari impegni (partecipazione a processi, visite o terapie mediche, impegni familiari, ecc.), permessi per assistenza ai figli (legge 151/2001)
- Dati sensibili per richieste, certificazioni, dichiarazioni e concessioni relativi a stato di gravidanza e al rischio di aborto o interdizione o astensione o riduzione orario per allattamento
- Dati comuni e sensibili per richieste e concessioni relativi part-time
- Dati sensibili per trasmissione di concessioni, permessi, congedi, aspettative e simili a Enti pubblici di controllo quali Ragioneria dello Stato, ecc.

Carriera, Nomine, Graduatorie, ecc.

- Dati comuni relativi all'organico, ai trasferimenti e alle utilizzazioni
- Dati sensibili per richieste,certificazioni, dichiarazioni e concessioni su particolari situazioni personali o familiari che danno diritto a punteggi o preferenze o per utilizzo facilitazioni di graduatoria o di punteggio per trasferimento e Grandi invalidi di guerra (art. 38 l.448/1999)
- Dati comuni contenuti nel contratto di assunzione
- Dati comuni per richieste, certificazioni, dichiarazioni e concessioni per immissione in ruolo, ricostruzione di carriera, ricongiungimenti di periodi assicurativi e riscatto di periodi a fini pensionistici
- Dati sensibili relativi al periodo di prova, note di merito o demerito, provvedimenti disciplinari
- Dati sensibili e giudiziari per cessazione o dispensa dal servizio dovuti a cause particolari quali inidoneità fisica, incapacità o persistente insufficiente rendimento, destituzione per motivi disciplinari , per reati, dispensa dal servizio per esito sfavorevole della prova
- Dati sensibili relativi alla tutela dei dipendenti in particolari condizioni psicofisiche (art. 124 DPR 309/90)
- Dati sensibili relativi alle pratiche per riconoscimento di invalidità per causa di servizio
- Dati comuni e sensibili di persone aspiranti alla supplenza o all'insegnamento contenute in documenti quali domande, dichiarazioni, certificazioni, curriculum per inserimento in graduatorie
- Dati comuni contenuti negli elenchi di persone aspiranti alla supplenza o all'insegnamento e pubblicati anche su reti di comunicazione elettronica
- Dati comuni e sensibili riguardante la nomina e gestione carriera del Docente di Religione
- Dati comuni contenuti nelle pratiche per le nomine dei commissari d'esami, anche mediante via telematica (dati comuni)
- Dati sensibili contenuti in documenti prodotti per fini contrattuali riguardante certificati di buona condotta, certificati di sana e robusta costituzione,, dichiarazione sui carichi pendenti nel casellario giudiziario

Rapporti economici, previdenziali, fiscali

- Dati comuni relativi agli incentivi economici su fondo d'Istituto e in genere
- Dati sensibili riguardante la documentazione da trasmettere al CAF per il mod. 730, contenente notizie sul reddito annuo e sul patrimonio, sul conferimento dell'8 per mille a chiese od organizzazioni religiose
- Dati sensibili relativi ai lavoratori a tempo determinato riguardante la gestione della retribuzione con documenti cartacei: calcolo stipendio, cedolino stipendio, prospetti di spesa, scheda fiscale interna, modello 101, inserimento di assenze e scioperi che comportano riduzione di stipendio, ritenute per delega sindacale e altre ritenute, gestione fiscale come detrazioni e gestione previdenziale, gestione richieste e attribuzioni delle detrazioni fiscali anche per dipendenti a tempo indeterminato
- Dati sensibili relativi a richieste, certificazioni , dichiarazioni e concessioni relativamente a benefici di natura economica, Assegno per Nucleo Familiare (art. 2 legge153/1988)
- Dati comuni relativi alla gestione e trasmissione all'INPDAP per via cartacea del progetto di liquidazione TFR per ogni dipendente a tempo determinato
- Dati sensibili relative alle domande di prestiti, cessione del quinto ecc.
- Dati sensibili per denuncia infortuni
- Dati sensibili per pignoramenti dello stipendio e di ritenute per eventuali danni erariali
- Dati sensibili relativi alla trasmissione al Tesoro per via cartacea dei compensi accessori a fine del conguaglio fiscale
- Dati sensibili relativi a qualunque pratica connessa alla gestione del dipendente relativamente allo stato retributivo, fiscale, previdenziale e amministrativo.

Sindacali

- Dati sensibili relativi alla dichiarazione di iscrizione a un sindacato con delega al versamento mensile dei contributi, gestione diretta delle ritenute sindacali o trasmissione al Tesoro per via cartacea
- Dati sensibili relativi alle dichiarazione di adesione a sciopero e registrazione dell'assenza per sciopero
- Dati sensibili relativi ai permessi per assemblea sindacale
- Dati sensibili relativi alla trasmissioni al Ministero del Tesoro per via cartacea delle ritenute per sciopero
- Dati sensibili inerenti procedure sindacali, circolari, proclamazioni di sciopero, gestione contratto integrativo della scuola, rapporti con RSU e sindacati
- Dati sensibili per richieste, certificazioni, dichiarazioni e concessioni in relazione a permessi e distacchi per attività sindacali
- Dati sensibili per rapporti con Rappresentante dei Lavoratori per la Sicurezza

Varie

- dati comuni relativi all'orario di insegnamento di tutti i docenti, con comunicazione anche ad altre scuole per i docenti "a scavalco"
- dati comuni relativi alla convocazione di riunioni, consigli di classe, collegio docenti, scrutini ecc., con comunicazione anche ad altre scuole per i docenti "a scavalco"
- dati sensibili per richieste e concessioni di autorizzazione a svolgere altre attività lavorative per persone in part-time e di svolgimento di attività libero-professionale
- dati sensibili contenuti nelle cartelle sanitarie ai sensi del D.lgs 81/08 ed eventuale giudizio di idoneità o inidoneità al lavoro, corrispondenza con dipendenti su particolari situazioni personali o professionali
- dati sensibili relativi ad eventuali controversie di lavoro
- dati sensibili e giudiziari relativi ad eventuali denunce per violazioni civili e penali
- dati sensibili relative a pratiche di dipendenti che usufruiscano di permessi o aspettative perché ricoprono cariche pubbliche o politiche
- dati comuni relativi alla partecipazione di corsi e convegni o e relative autorizzazioni
- dati comuni relativi ai prodotti dal collegio docenti e dalle commissioni di lavoro formate da docenti

Modalità di trattamento

- I fascicoli personale sono costituiti da documenti cartacei e conservati in archivi non elettronici all'interno degli uffici preposti, come indicato nella sezione relativa all'elenco degli archivi
- I fascicoli relativi al personale al termine del rapporto di lavoro sono depositati in storico
- I fascicoli contenenti dati sensibili o personali sono conservati separatamente
- I dati prodotti con strumenti elettronici sono conservati in archivi elettronici e in archivi non elettronici qualora venissero prodotti anche i corrispondenti documenti cartacei e trasmessi all'occorrenza per via telematica agli archivi remoti del Ministero dell'Istruzione
- La gestione dei dati e delle pratiche relative al personale sono trattate con strumenti cartacei e strumenti elettronici, caratterizzati da funzioni come indicato nelle misure minime di sicurezza descritte in questo documento e in conformità all'allegato B parte A del D.LGS. 196/03
- Gli atti relativi alla produzione di certificati o documenti sono prodotti con strumenti elettronici quali software Microsoft Office (Word, Excel, ecc.) e depositati in archivi elettronici e cartacei come indicato nella sezione relativa all'elenco degli archivi
- I dati contenuti in documenti trasmessi al CAF sono conservati in busta chiusa
- I dati sensibili contenuti nelle cartelle sanitarie ai sensi del D.lgs 81/08 sono custoditi in busta chiusa

Archivi non elettronici

- Archivio corrente docenti (contiene Fascicoli Personali)
- Archivio storico docenti (contiene Fascicoli Personali)
- Archivio registri, prospetti e graduatorie
- Archivio di corrispondenza generale (esclusa le corrispondenze con singoli che dispongano di Fascicolo Personale)
- Archivio corrente assenze
- Archivio assenze storico
- Archivio stipendi, previdenziali, ecc. corrente
- Archivio stipendi, previdenziali, ecc. storico
- Affari generali docenti
- Affari generali docenti storico

Archivi elettronici :

- Archivio ARGO-SIDI personale
- Archivio ARGO-SIDI retribuzioni
- Archivio documenti elettronici 1 redatti con sw M.Office

Elenco dati trattati con strumenti elettronici:

- Gestione dati comuni e sensibili relativi all'amministrazione del personale area ARGO-SIDI personale
- Gestione liquidazione competenze mediante area ARGO-SIDI retribuzioni
- Dati comuni e sensibili in documenti generici, certificati e pratiche redatti con programma di Office Automation (Microsoft Office)
- Dati comuni e sensibili per la gestione e la trasmissione per via telematica al MIUR o altri enti di competenza relativi all'assunzione in servizio
- Dati comuni contenuti nelle pratiche per le nomine dei commissari d'esami, anche mediante via telematica
- Dati comuni e sensibili relativi ai lavoratori a tempo determinato riguardante la gestione della retribuzione con documenti con programma informatico ARGO-SIDI : calcolo stipendio, cedolino stipendio, prospetti di spesa, scheda fiscale interna, modello 101, inserimento di assenze e scioperi che comportano riduzione di stipendio, ritenute per delega sindacale e altre ritenute,

gestione fiscale e gestione previdenziale, gestione richieste e attribuzioni delle detrazioni fiscali anche per dipendenti a tempo indeterminato, gestione trattamenti di missione

- Dati sensibili relativi alla trasmissione al Tesoro per via telematica dei compensi accessori a fine del conguaglio fiscale
- Dati sensibili relativi alla trasmissioni al Ministero del Tesoro per via telematica delle ritenute per sciopero
- Dati comuni e sensibili contenuti in comunicazioni per via telematica o posta elettronica ad altre scuole o da altre scuole di assunzione in servizio, di assenze, di particolari concessioni e di altri atti nel caso di docenti utilizzati a scavalco da più scuole, orario scolastico, di impegni per riunioni, ecc., di partecipazione ad esami ed altri attività.
- Dati comuni e sensibili contenuti in comunicazioni per via telematica o posta elettronica al MIUR o ad altre scuole per graduatorie
- Dati comuni di elenchi anagrafici contenenti dati comuni prodotti con documenti elettronici redatti mediante sw Office, trasmessi per via telematica, per posta elettronica o memorizzati su supporti di memorizzazione elettronici, trasmessi ad enti esterni quali ASL, enti pubblici, aziende e privati in occasione di visite guidate, viaggi e simili.
- Dati comuni e sensibili per trasmissione per via telematica ad enti pubblici (Ministero del Tesoro, MIUR, CSA, Uffici scolastici Regionali, INPDAP, INPS, INAIL, Ministero Finanze, Ragioneria dello Stato) per comunicazione di dati per graduatorie, assunzione e contratto di lavoro, gestione stipendi, andamento in quiescenza e TFR, attività previdenziale, adempimenti fiscali (ivi compreso anagrafica delle retribuzioni)
- Dati comuni e sensibili per trasmissione per via telematica a INAIL e Questura per denuncia infortuni

- ***Elenco dati comunicati a strutture esterne***:

- Dati comuni e sensibili relativi al trasferimento trasmessi ad altra scuola pubblica, comprendente documenti quali foglio notizie e parte del Fascicolo Personale (documenti anagrafici, documenti scolastici di attualità, mentre eventuali certificati medici e altri dati sensibili o giudiziari soltanto su consenso dell'interessato)
- Dati comuni e sensibili relativi al trasferimento trasmessi ad altra scuola pubblica ad altre scuole o da altre scuole di assunzione in servizio, di assenze, di particolari concessioni e di altri atti nel caso di docenti utilizzati a scavalco da più scuole, di orario scolastico, di impegni per riunioni, ecc., di partecipazione ad esami ed altri attività
- Dati comuni relativi alle graduatorie trasmessi ad altra scuola
- Dati comuni di elenchi anagrafici contenenti dati comuni prodotti con documenti elettronici redatti mediante sw Office, trasmessi per via telematica, per posta elettronica o memorizzati su supporti di memorizzazione elettronici, trasmessi ad enti esterni quali ASL, enti pubblici, aziende e privati in occasione di visite guidate, viaggi e simili.
- Dati sensibili riguardante la documentazione da trasmettere al CAF per il mod. 730, contenente notizie sul reddito annuo e sul patrimonio, sul conferimento dell'8 per mille a chiese od organizzazioni religiose
- Dati sensibili relative alle domande di prestiti, cessione del quinto trasmessi a enti pubblici
- Dati sensibili relativi alla trasmissione ad enti pubblici di particolari pratiche, su richiesta del dipendente, per ottenere determinati benefici
- Dati sensibili relativi alla trasmissione al Tesoro per via cartacea dei compensi accessori a fine del conguaglio fiscale
- Dati sensibili relativi alla trasmissione al Tesoro delle ritenute sindacali da operare
- Dati sensibili relativi alla trasmissione ad enti pubblici (Ministero del Tesoro, MIUR, CSA, Uffici scolastici Regionali, INPDAP, INPS, INAIL, Ministero Finanze, Ragioneria dello Stato) per comunicazione di dati per graduatorie, assunzione e contratto di lavoro, gestione stipendi, andamento in quiescenza e TFR, attività previdenziale, adempimenti fiscali (ivi compreso anagrafica delle retribuzioni). Dati sensibili relativi alla trasmissione a Inail e Questura per denuncia infortuni
- Dati sensibili relativi alla trasmissione a enti pubblici nel caso di dipendenti che usufruiscano di permessi o aspettative perché ricoprono cariche pubbliche

- Dati sensibili relativi alla trasmissione a enti pubblici nel caso di dipendenti che usufruiscano di permessi o aspettative perché ricoprono cariche pubbliche
- Dati comuni pubblicati e disponibili per consultazione o diffusione mediante albo delle graduatorie e di una serie di atti, quali partecipazione di docenti a commissioni, ripartizione del fondo incentivante, ecc.

Categoria di trattamenti operati (indicati nella Tabella 4 **– Strutture preposte al trattamento:**

Descrizione	*ID Trattamento*	*n. progressivo*	*Tipo trattamento (1)*	*Tipo dato (2)*
dati dipendenti e loro famiglie per l'attività amministrativa	T3	1	CE	CS
dati dipendenti e loro famiglie relativi alla retribuzione, previdenza	T3	2	CE	CS
dati dipendenti per le attività riguardanti la didattica	T3	3	CE	CS
dati dipendenti relativi a pratiche di assicurazione, gestione infortuni e malattie professionali, di inabilità al lavoro e simili	T3	4	CE	CS
dati dipendenti relative ad attività sindacali	T3	5	CE	CS

(1) *C: cartaceo*

E: elettronico

(2) *C: dati comuni*

S: dati sensibili

G: dati giudiziari

T4 - Collaborazioni professionali esterne. Dati personali trattati da Assistenti Amministrativi, DSGA e dal Dirigente Scolastico

Tipologia di dati:

- Dati comuni e sensibili relativi a curriculum e offerte di prestazioni contenenti dati personali quali, profilo culturale, relazioni, interessi
- Dati comuni e sensibili inerenti documenti e comunicazioni con l'interessato
- Dati comuni e sensibili inerenti trasmissioni telematiche o con posta elettronica dei dati personali di collaboratori esterni relativamente alle prestazioni economiche ad enti preposti
- Dati comuni dei collaboratori esterni relativi a rapporti inerenti la contabilità

Modalità di trattamento

- La trasmissione con strumenti cartacei o elettronici di dati di collaboratori esterni riguardanti dati della sfera personale, ad organizzazioni esterne, avviene solo su consenso dell'interessato
- I dati prodotti con strumenti elettronici sono conservati in archivi elettronici come indicato nella sezione relativa all'elenco degli archivi

Archivi non elettronici

- Archivio corrente collaboratori esterni
- Archivio storico collaboratori esterni
- Archivio corrente fornitori
- Archivio storico fornitori
- Archivio corrente connesso alla gestione del Bilancio.
- Archivio storico connesso alla gestione del Bilancio.

Archivi elettronici :

- Archivio ARGO-SIDI bilancio
- Archivio ARGO-SIDI retribuzioni
- Archivio ARGO-SIDI minute spese
- Archivio documenti elettronici 1 redatti con sw M.Office 1

Elenco dati trattati con strumenti elettronici:

- Gestione dati comuni e sensibili relativi all'amministrazione dei rapporti con collaboratori esterni mediante l'impiego delle aree ARGO-SIDI bilancio, retribuzioni, minute spese
- Dati comuni e sensibili in documenti generici, certificati, pratiche, preventivi, fatture, onorari, note di spesa redatti con programma di Office Automation (Microsoft Office)
- Dati comuni e sensibili inerenti trasmissioni telematiche o con posta elettronica ad enti preposti dei dati personali di collaboratori esterni relativamente alle prestazioni economiche
- Dati contenuti nella comunicazione con collaboratori esterni mediante l'impiego di trasmissione telematiche o posta elettronica

Elenco dati comunicati a strutture esterne:

- Dati contenuti nella comunicazione con collaboratori esterni mediante l'impiego di trasmissione telematiche o posta elettronica
- Dati comuni e sensibili inerenti trasmissioni telematiche o con posta elettronica ad enti preposti dei dati personali di collaboratori esterni relativamente alle prestazioni economiche

Categoria di trattamenti operati (indicati nella Tabella 4 **– Strutture preposte al trattamento:**

Descrizione	*ID Trattamento*	*n. progressivo*	*Tipo trattamento (1)*	*Tipo dato (2)*
dati dei collaboratori esterni per l'attività amministrativa, retributiva, previdenziale , fiscale e tutti gli altri ARGOmenti connessi alla categoria	T4	1	CE	CS

(1) *C: cartaceo*

E: elettronico

(2) *C: dati comuni*

S: dati sensibili

G: dati giudiziari

T5 - Beni e servizi: acquisti, affitti, vendite. Dati personali trattati da Assistenti Amministrativi, DSGA e dal Dirigente Scolastico

Tipologia di dati:

- Dati comuni relativi alla gestione degli acquisti e delle vendite di beni e servizi, nonché di affitti e prestazioni quali offerte, preventivi, referenze, redazione di relazioni e prospetti comparativi delle offerte, ordini di acquisto, fatture, contratti, collaudi.
- Dati comuni relativi a prestazioni, servizi, forniture ad altre scuole, nonché introiti per affitto locali quali laboratori, sale per conferenze, spazi per macchinette automatiche distributrici, ecc.
- Dati comuni e sensibili inerenti documenti e comunicazioni con l'interessato al contratto dei beni e servizi
- Dati comuni degli interessati al contratto dei beni e servizi inerenti la contabilità
- Dati comuni relativi alla gestione dell'inventario della scuola e dei beni di proprietà dell'ente locale
- Dati comuni relativi alla gestione di preventivi per acquisti di beni e servizi, anche tramite l'impiego di trasmissione per via telematica del Programma di Razionalizzazione della Spesa per Beni e Servizi della P.A.
- Dati comuni relativi alla gestione della biblioteca

Modalità di trattamento

- I dati relativi alla gestione dei beni e servizi sono raccolti in fascicoli e conservati in archivi non elettronici
- I dati prodotti con strumenti elettronici sono conservati in archivi elettronici e in archivi non elettronici qualora venissero prodotti anche i corrispondenti documenti cartacei

Archivi non elettronici

- Archivio corrente fornitori
- Archivio storico fornitori
- Archivio corrente connesso alla gestione del Bilancio
- Archivio storico connesso alla gestione del Bilancio

Archivi elettronici :

- Archivio ARGO-SIDI bilancio
- Archivio ARGO-SIDI retribuzioni
- Archivio ARGO-SIDI minute spese
- Archivio documenti elettronici 1 redatti con sw M.Office 1

Elenco dati trattati con strumenti elettronici:

- Dati comuni e sensibili in documenti generici, certificati, pratiche, preventivi, fatture, note di spesa redatti con programma di Office Automation (Microsoft Office)
- Gestione dati comuni e sensibili relativi all'amministrazione dei rapporti con collaboratori esterni mediante l'impiego delle aree ARGO-SIDI bilancio, retribuzioni, minute spese
- Dati contenuti nella comunicazione con gli interessati al contratto di beni e servizi mediante l'impiego di trasmissione telematiche o posta elettronica
- Dati comuni relativi alla gestione di preventivi per acquisti di beni e servizi, anche tramite l'impiego di trasmissione per via telematica del Programma di Razionalizzazione della Spesa per Beni e Servizi della P.A.

Elenco dati comunicati a strutture esterne:

- Dati contenuti nella comunicazione con gli interessati al contratto di beni e servizi mediante l'impiego di trasmissione telematiche o posta elettronica
- Dati comuni relativi alla gestione di preventivi per acquisti di beni e servizi, anche tramite l'impiego di trasmissione per via telematica del Programma di Razionalizzazione della Spesa per Beni e Servizi della P.A.

Categoria di trattamenti operati (indicati nella Tabella 4 **– Strutture preposte al trattamento:**

Descrizione	*ID Trattamento*	*n. progressivo*	*Tipo trattamento (1)*	*Tipo dato (2)*

dati amministrativi, fiscali e tutti gli altri ARGOmenti connessi alla gestione dei beni e servizi	T5	1	CE	C

(1) *C: cartaceo*

E: elettronico

(2) *C: dati comuni*

S: dati sensibili

G: dati giudiziari

T6 - Gestione finanziaria e del bilancio. Dati personali trattati da Assistenti Amministrativi, DSGA e dal Dirigente Scolastico

Tipologia di dati:

- Dati comuni relativi alla gestione del Bilancio Preventivo e del Conto Consuntivo quali mandati, ordinativi di pagamento, rapporti con banche e l'Istituto Cassiere e relativa trasmissione alle organizzazioni di competenza
- Dati comuni relativi a delibere del Consiglio d'Istituto e della Giunta Esecutiva
- Dati comuni e sensibili relativi alla gestione assicurazioni
- Dati comuni e sensibili relativi alla gestione versamenti Irpef e fiscali in genere, previdenziali, ecc.
- Dati comuni relativi alla gestione e trasmissione degli stessi in rapporto con i revisori dei conti
- Dati comuni e sensibili inerenti documenti e comunicazioni per corrispondenza operativa redatti anche con programma di Office Automation (Microsoft Office)
- Dati comuni inerenti la contabilità

Modalità di trattamento

- I dati relativi alla gestione dei beni e servizi sono raccolti in fascicoli e conservati in archivi non elettronici
- I dati prodotti con strumenti elettronici sono conservati in archivi elettronici e in archivi non elettronici qualora venissero prodotti anche i corrispondenti documenti cartacei

Archivi non elettronici

- Archivio corrente fornitori
- Archivio storico fornitori
- Archivio corrente Stipendi
- Archivio storico Stipendi
- Archivio corrente connesso alla gestione del Bilancio
- Archivio storico connesso alla gestione del Bilancio
- Registri e atti del Consiglio d'Istituto e della Giunta Esecutiva

Archivi elettronici :

- Archivio ARGO-SIDI bilancio
- Archivio ARGO-SIDI retribuzioni
- Archivio ARGO-SIDI minute spese
- Archivio documenti elettronici 1 redatti con sw M.Office
- Archivio documenti contabili

- ***Elenco dati trattati con strumenti elettronici***:

  - Dati comuni e sensibili in documenti generici, certificati, pratiche, preventivi, fatture, note di spesa redatti con programma di Office Automation (Microsoft Office)
  - Gestione dati comuni e sensibili relativi all'amministrazione mediante l'impiego delle aree ARGO-SIDI bilancio, retribuzioni, minute spese e sw Sysdata
  - Dati contenuti in documenti inerenti la gestione finanziaria e del bilancio quali offerte, preventivi , fatture, onorari, note spese, e di corrispondenza operativa con gli interessati coinvolti mediante l'impiego di trasmissione telematiche o posta elettronica

- ***Elenco dati comunicati a strutture esterne***:

  - Dati contenuti in documenti inerenti la gestione finanziaria e del bilancio quali offerte, preventivi , fatture, onorari, note spese, e di corrispondenza operativa con gli interessati coinvolti mediante l'impiego di trasmissione telematiche o posta elettronica

Categorie di trattamenti operati (indicati nella Tabella 4 **– Strutture preposte al trattamento:**

Descrizione	*ID Trattamento*	*n. progressivo*	*Tipo trattamento (1)*	*Tipo dato (2)*
dati connessi alla gestione del bilancio e tutti gli ARGOmenti connessi, compresi i rapporti con le banche e l'Istituto Cassiere	T6	1	CE	CS

(1) *C: cartaceo*

E: elettronico

(2) *C: dati comuni*

S: dati sensibili

G: dati giudiziari

T7 - Gestione Istituzionale, Protocollo e Posta. Dati personali trattati da Assistenti Amministrativi, DSGA e dal Dirigente Scolastico

Tipologia di dati:

- Dati comuni e sensibili relativi a tutti i documenti in ingresso e in uscita quest'ultimi redatti anche con programma di Office Automation (Microsoft Office) ovvero provenienti anche per via telematica da organizzazioni, enti, aziende e persone fisiche esterne
- Dati comuni e sensibili contenuti in messaggi di posta elettronica

Modalità di trattamento

- Tutti i documenti in ingresso e in uscita vengono protocollati, tranne quelli sottoposti al protocollo riservato che sarà gestito dal Dirigente Scolastico. I documenti protocollati vengono passati all'Incaricato che deve trattare la pratica, che si occupa anche dell'archiviazione o della spedizione. Tuttavia documenti di valenza istituzionale perpetua o pluriennale sono archiviati a parte. Fanno parte dello stesso trattamento i documenti cartacei prodotti mediante trasmissione per via telematica.
- I dati relativi alla gestione dei istituzionale, protocollo e posta sono raccolti in fascicoli e conservati in archivi non elettronici
- I dati prodotti con strumenti elettronici sono conservati in archivi elettronici e in archivi non elettronici qualora venissero prodotti anche i corrispondenti documenti cartacei

Archivi non elettronici

- Archivio protocollo cartaceo
- Archivio corrente generale
- Archivio storico generale
- Archivio corrente Riservato (Cassaforte del Dirigente scolastico)
- Archivio storico Riservato (Cassaforte del Dirigente scolastico)
- Registri e atti del Consiglio d'Istituto e della Giunta Esecutiva

Archivi elettronici :

- Archivi posta elettronica
- Archivio documenti elettronici 1 redatti con sw M.Office

Elenco dati trattati con strumenti elettronici:

- Dati comuni e sensibili relativi a tutti i documenti in ingresso e in uscita quest'ultimi redatti anche con programma di Office Automation (Microsoft Office) ovvero provenienti anche per via telematica da organizzazioni, enti, aziende e persone fisiche esterne
- Dati comuni e sensibili relativi a tutti i documenti in ingresso e in uscita quest'ultimi redatti con programma di Office Automation (Microsoft Office) e trasmessi o ricevuti per posta elettronica anche provenienti anche per via telematica da organizzazioni, enti, aziende e persone fisiche esterne

Elenco dati comunicati a strutture esterne:

- Dati comuni e sensibili relativi a tutti i documenti in ingresso e in uscita questi ultimi redatti anche con programma di Office Automation (Microsoft Office) ovvero provenienti anche per via telematica o posta elettronica da organizzazioni, enti, aziende e persone fisiche esterne

- Dati comuni e sensibili relativi a tutti i documenti in ingresso e in uscita questi ultimi redatti con programma di Office Automation (Microsoft Office) e trasmessi o ricevuti per posta elettronica anche provenienti anche per via telematica da organizzazioni, enti, aziende e persone fisiche esterne

Categorie di trattamenti operati (indicati nella Tabella 4 **– Strutture preposte al trattamento:**

Descrizione	*ID Trattamento*	*n. progressivo*	*Tipo trattamento (1)*	*Tipo dato (2)*
protocollo ordinario	T7	1	CE	CS
protocollo riservato	T7	2	C	CS
affari generali	T7	3	CE	CS

(1) *C: cartaceo*

E: elettronico

(2) *C: dati comuni*

S: dati sensibili

G: dati giudiziari

T8 - Gestione di trattamenti da parte di persone, anche esterne alla scuola, facenti parte degli organi collegiali

Tipologia di dati:

- Dati comuni di alunni, genitori, docenti e personale della scuola
- Dati comuni e sensibili contenuti in verbali e delibere prodotti dal Consiglio di Istituto anche utilizzando anche programmi di Office Automation (Microsoft Office)
- Dati comuni contenuti nella corrispondenza fra il presidente del Consiglio di Istituto e i membri, quali notizie sulla convocazione e riunioni

Modalità di trattamento

- Il presidente del CdI convoca le riunioni dell'organo e può mandare della corrispondenza alle famiglie e agli alunni
- Alcuni membri del CdI o del consiglio hanno il compito di redigere verbali e atti cartacei utilizzando anche programmi di Office Automation (Microsoft Office)
- I membri possono sottoscrivere delibere del CdI o di classe

Archivi non elettronici

- Archivio corrente delibere di CdI e GE
- Archivio storico delibere di CdI e GE
- Registri dei verbali dei Consigli di classe, dei CdI e della GE

- ***Archivi elettronici*** : nessuno
- ***Elenco dati trattati con strumenti elettronici***:

  - Dati comuni e sensibili contenuti in verbali e delibere prodotti dal Consiglio di Istituto anche utilizzando anche programmi di Office Automation (Microsoft Office)

- ***Elenco dati comunicati a strutture esterne***:

  - Dati comuni contenuti nella corrispondenza fra il presidente del Consiglio di Istituto e i membri, quali notizie sulla convocazione e riunioni

Categorie di trattamenti operati (indicati nella Tabella 4 **– Strutture preposte al trattamento:**

Descrizione	*ID Trattamento*	*n. progressivo*	*Tipo trattamento (1)*	*Tipo dato (2)*
delibere e atti del CdI e GE	T8	1	CE	CS

(1) *C: cartaceo*

E: elettronico

(2) *C: dati comuni*

S: dati sensibili

G: dati giudiziari

T9 - Gestione Trattamenti di dati personali effettuati da Collaboratori Scolastici e Personale Ausiliario

- ***Tipologia di dati:***

  - Dati comuni di alunni, docenti personale della scuola contenuti in qualunque tipologia di documenti anche in collaborazione con altri incaricati

- ***Modalità di trattamento***

  - I collaboratori e il personale ausiliario incaricati possono: ricevere, trasportare, consegnare, inviare documenti contenenti dati comuni, aperti o sensibili collocati in busta chiusa, tra cui registri; visionare documenti contenenti dati comuni allo scopo di dare indicazioni di massima agli utenti; custodire documenti e registri per brevi periodi; gestire dati comuni in elenchi di alunni, dipendenti e genitori per attività varie della scuola; fotocopiare e faxare documenti

contenenti dati comuni; collaborare ad operazioni di archiviazione di documenti cartacei; collaborare ad operazioni di scarto ed eliminazione di documenti cartacei; in generale, svolgere attività di supporto a tutti i trattamenti svolti nella scuola

- ***Archivi non elettronici***
  - In generale qualunque archivio gestito in collaborazione con altri incaricati
- ***Archivi elettronici*** : nessuno
- ***Elenco dati trattati con strumenti elettronici***: nessuno
- ***Elenco dati comunicati a strutture esterne***:
  - Spedizione o consegna di plichi predisposti dalla segreteria o dal Dirigente
- **Categorie di trattamenti operati (indicati nellaTabella 4** – Strutture preposte al trattamento:

Descrizione	*ID Trattamento*	*n. progressivo*	*Tipo trattamento (1)*	*Tipo dato (2)*
Dati comuni di alunni, docenti personale della scuola contenuti in qualunque tipologia di documenti anche in collaborazione con altri incaricati	T9	1	C	C

(1) *C: cartaceo*

E: elettronico

(2) *C: dati comuni*

S: dati sensibili

G: dati giudiziari

T10 - Gestione Trattamenti di dati personali effettuati dall'amministratore di rete

- ***Tipologia di dati:***
  - Tutti i dati trattati con strumenti elettronici contenuti negli archivi con finalità di manutenzione e configurazione degli apparati, del software, del sistema di autorizzazione e dei sistemi di sicurezza in genere
  - Gestione delle credenziali di autenticazione e delle parole chiave
  - Gestione delle chiavi per la crittografia

- ***Modalità di trattamento***

  - Il trattamento dei dati avviene in seguito ad interventi sui sistemi elettronici contenenti dati personali. Tale operazione avviene in seguito ad una segnalazione dell'incaricato o a seguito di malfunzionamenti rilevati direttamente dall'amministratore di sistema. Le produzioni di parole chiave, password, credenziali di autenticazione e chiave di crittografia sono compiti affidati all'amministratore di sistema il quale consegnerà, in busta chiusa, tali informazioni all'incaricato in modo che possa accedere ai dati elettronici di sua competenza e al DSGA per l'archiviazione

- ***Archivi non elettronici***

  - nessuno

- ***Archivi elettronici*** : tutti
- ***Elenco dati trattati con strumenti elettronici***: tutti
- ***Elenco dati comunicati a strutture esterne***:

  - Se l'amministratore di sistema è un'organizzazione esterna (azienda, esperto, ecc.) saranno gestiti i dati personali relativi alle parole chiave, credenziali di autenticazione, chiave di crittografia. Inoltre sono anche gestiti tutti i dati contenuti in archivi elettronici trattati per esigenze relative alla funzionalità dei sistemi elettronici

- **Categorie di trattamenti operati (indicati nella Tabella 4** – Strutture preposte al trattamento:

Descrizione	*ID Trattamento*	*n. progressivo*	*Tipo trattamento (1)*	*Tipo dato (2)*
Dati comuni e sensibili degli archivi elettronici, chiavi di autenticazione, crittografia, password, credenziali di autenticazione	T10	1	E	CSG

(1) *C: cartaceo*

E: elettronico

(2) *C: dati comuni S: dati sensibili G: dati giudiziari*

Allegato 2: Misure di protezione dei dati personali

I dati personali dovranno essere trattati secondo le specifiche generali previste del D.LGS. 196/03 e in base alle istruzioni individuate nel presente documento. Ciascuna struttura di riferimento e i relativi incaricati

dovranno rispettare le istruzioni a loro assegnate. Nella tabella seguente sono riassunte le istruzioni e le strutture di riferimento a cui esse sono applicate. Le stesse istruzioni sono descritte dettagliatamente in seguito

Struttura di riferimento	*Tipo Trattamento (1)*	*Descrizione procedura di protezione dati (PPD)*	*ID procedura di protezione dati*
Tutte	G	Regole Generali artt. 31-34-35 D.LGS. 196/03	PPD00
Assistenti Amministrativi e DSGA, Collaboratori Scolastici per quanto di loro pertinenza.	C	Trattamento dei documenti (in ingresso, uscita, ecc.)	PPD01
Assistenti Amministrativi e DSGA	C	Informativa per la raccolta di dati personali	PPD02
Assistenti Amministrativi e DSGA	C	Sottoscrizione dell'interessato e deleghe	PPD03
Assistenti Amministrativi e DSGA	C	Trasferimenti, abbandoni, cessazioni contratti, conclusione degli studi	PPD04
Assistenti Amministrativi e DSGA	C	Regole generali per la sicurezza degli archivi	PPD05
Assistenti Amministrativi e DSGA	C	Conservazione di registri e altri documenti utilizzati per anni scolastici precedenti e non più utilizzati	PPD06
Assistenti Amministrativi e DSGA	C	Scarto periodico dei documenti	PPD07
Assistenti Amministrativi e DSGA	C	Distruzione dei documenti	PPD08
Assistenti Amministrativi e DSGA, Collaboratori Scolastici per quanto di loro pertinenza.	C	Documenti provvisori	PPD09
Assistenti Amministrativi e DSGA, Collaboratori Scolastici per quanto di loro pertinenza.	C	Fotocopiatura	PPD10
Assistenti Amministrativi e DSGA, Collaboratori Scolastici per quanto di loro pertinenza.	C	Utilizzo documenti da parte di terzi	PPD11

Struttura di riferimento	*Tipo Trattamento (1)*	*Descrizione procedura di protezione dati (PPD)*	*ID procedura di protezione dati*
Assistenti Amministrativi e DSGA, Collaboratori Scolastici per quanto di loro pertinenza.	C	Accesso in uffici da terzi (dati cartacei)	PPD12
Assistenti Amministrativi, DSGA, Amministratore di sistema	E	Sistema di autenticazione e autorizzazione	PPD13
Assistenti Amministrativi, DSGA, Amministratore di sistema	E	Sistema di cifratura dei dati idonei a rivelare lo stato di salute e la vita sessuale	PPD14
Assistenti Amministrativi, DSGA, Amministratore di sistema	E	Protezione da accessi telematici dannosi	PPD15
Assistenti Amministrativi, DSGA, Amministratore di sistema	E	Uso dei supporti rimovibili	PPD16
Assistenti Amministrativi, DSGA, Amministratore di sistema	E	Accesso in uffici da terzi (dati elettronici)	PPD17
Docenti	C	Registri	PPD18
Docenti, Assistenti Amministrativi, DSGA	C	Certificazioni mediche e informazioni sullo stato di salute degli alunni	PPD19
Docenti	C	Elaborati contenenti notizie particolari o sensibili	PPD20
Docenti, Assistenti Amministrativi, DSGA	C	Gestione degli elenchi degli alunni	PPD21
Docenti, Assistenti Amministrativi e DSGA, Collaboratori Scolastici per quanto di loro pertinenza.	C	Documenti scolastici contenenti dati personali	PPD22
Membri Organi Collegiali	C	Documenti, verbali, atti e delibere degli O.C.	PPD23
Collaboratori Scolastici e del Personale Ausiliario	C	Documenti scolastici gestiti dai collaboratori scolastici e dal personale ausiliario	PPD24
Collaboratori Scolastici e del Personale Ausiliario	C	Trasporto di documenti scolastici	PPD25

Struttura di riferimento	*Tipo Trattamento (1)*	*Descrizione procedura di protezione dati (PPD)*	*ID procedura di protezione dati*
Collaboratori Scolastici e del Personale Ausiliario	C	Custodia uffici	PPD26

(1) G: Istruzioni generali C: cartaceo E: elettronico

Procedura PPD00: Istruzioni Generali: "Titolo V - Sicurezza dei dati e dei sistemi - Capo I – Misure di Sicurezza" del D.Lgs. 196/03

Art. 31. Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, 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, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 34. Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
   a) autenticazione informatica;
   b) adozione di procedure di gestione delle credenziali di autenticazione;
   c) utilizzazione di un sistema di autorizzazione;
   d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
   e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
   f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
   g) …; *(abrogata)*
   h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Art. *35. Trattamenti senza l'ausilio di strumenti elettronici*

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
   a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli Incaricati o alle unità organizzative;
   b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli Incaricati per lo svolgimento dei relativi compiti;
   c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli Incaricati.

Istruzioni per la sicurezza mediante strumenti non elettronici (supporti cartacei)

Procedura PPD01: trattamento dei documenti(in ingresso, uscita, ecc.)

Per "documenti in ingresso", si intendono i documenti o i supporti contenenti dati personali acquisiti dalla scuola ai fini di un loro impiego in trattamento. Per il trattamento dei documenti in ingresso valgono le seguenti regole:

1. Ogni documento cartaceo in ingresso ricevuto tramite posta o ricevuto in busta chiusa consegnata a mano viene di norma inviato all'ufficio protocollo dove sarà assegnato un protocollo e recapitata in genere alla dirigenza amministrativa o al dirigente scolastico. Fanno eccezione i documenti speciali dotati di particolare riservatezza che dovranno essere consegnati direttamente al Dirigente Scolastici che provvederà a protocollare il documento nel Registro di Protocollo Riservato e lo custodisce nella cassaforte Tabella **5 – Analisi dei rischi:**
2. (si veda Allegato 2). La cassaforte sarà chiusa a chiave e l'ufficio del Dirigente Scolastico sarà normalmente chiuso a chiave quando non presenziato dal Dirigente stesso. È facoltà del Dirigente Scolastico affidare compiti di trattamento ad un collaboratore incaricato
3. I dati contenuti nei documenti in ingresso possono essere trattati solo dagli incaricati su disposizione del Responsabile
4. L'incaricato deve verificare:

    - la provenienza dei documenti;
    - che tali documenti siano effettivamente necessari al trattamento in questione;
    - la tipologia dei dati contenuti (comuni, sensibili, , giudiziari o altri dati particolari), al fine di individuare le modalità legittime ed idonee per il trattamento e le misure di sicurezza da attuare;
    - l'osservanza del principio di pertinenza e non eccedenza rispetto o alle finalità del trattamento, la completezza, la correttezza e l'aggiornamento dei dati

5. Per documenti contenenti dati personali riferiti ad individui non ancora inseriti nelle procedure di trattamento di questa Istituzione, quali domande di ammissione, di iscrizione negli elenchi fornitori, ecc. a meno che non esistano già dei moduli predisposti, l'incaricato dovrà procedere a compilare l'informativa da consegnare all'interessato ai sensi dell'art. 22 del D.M. 196/03
6. L'Incaricato che riceve documenti recapitati personalmente o tramite un rappresentante autorizzato (compresi i corrieri privati), che contiene dati sensibili o giudiziari la cui tipologia non è prevista in nessuna delle procedure previste in questo documento, deve immediatamente metterli in busta chiusa se i documenti ne sono sprovvisti e recapitarli al responsabile di riferimento (DSGA o Dirigente Scolastico)

Per "documenti in uscita", si intendono i documenti o i supporti contenenti dati personali prodotti e rilasciati dalla scuola a soggetti esterni ad stessa. Nel caso di documenti in uscita è necessario all'atto della consegna o dell'invio, verificare che la persona che riceve il documento sia legittimata al ritiro e all'utilizzo (delega).

L'incaricato nello svolgere le operazioni di trattamento e di elaborazione di un documento deve seguire tutte le procedure atte a proteggere i dati contenuti come. In particolare:

<u>Per il trattamento manuale o con strumenti non elettronici:</u>

- Durante il trattamento è fatto obbligo conservare i documenti contenenti dati personali con discrezione
- Al termine del trattamento i documenti dovranno essere conservati all'interno degli appositi archivi muniti di serratura
- I dati sensibili e giudiziari sono trattati da incaricati negli uffici appositi riservati e separati dal luogo di accesso al pubblico. Lo sportello al pubblico dovrà riportare l'orario di apertura e l'indicazione di accedere una persona alla volta con l'obbligo di restare a distanza dalla persona che in quel momento è allo sportello

- In caso di allontanamento dal luogo dove vengono trattati i dati verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento. In caso di allontanamento momentaneo o per pause è necessario depositare i documenti in un cassetto chiuso a chiave anche provvisorio. Evitare di lasciare sui tavoli o comunque fuori dai contenitori documenti o fascicoli contenenti dati personali
- I dati non possono essere comunicati ad altri incaricati che trattano categorie di dati diversi senza specifica autorizzazione del titolare o del responsabile (ad esempio i dati trattati da un assistente amministrativo non possono essere comunicati ad un docente salvo per motivi ritenuti congrui da parte del rappresentante del titolare o dal responsabile)
- Al termine delle operazioni di trattamento è necessario conservare i documenti negli appositi contenitori e consegnare le chiavi al responsabile o all'incaricato di custodia delle chiavi

Per il trattamento con strumenti elettronici:

- Il DSGA sarà in possesso di una credenziale di autenticazione elettronica individuale costituita da uno più nomi utente e password
- L'accesso ai dati avverrà mediante la credenziale di autenticazione individuale utilizzando il dispositivo di accesso indicato nella Tabella 2
- Le credenziali di autenticazione consentiranno l'accesso a qualunque tipo di dato senza nessun limite
- I dati conservati sui dispositivi di memorizzazione dovranno essere conservati all'interno di appositi archivi muniti di serratura
- In caso di allontanamento dal dispositivo di accesso è necessario interdire la funzionalità mediante attivazione della maschera di richiesta delle credenziali di accesso
- Per problemi inerenti il buon funzionamento dei sistemi o per necessità di nuove configurazione contattare l'amministratore di rete.

Procedura PPD02: informativa per la raccolta di dati personali

Ai sensi dell'art. 18 del D.M. 196/03 all' Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG), quale ente pubblico non economico, è consentito trattare dati personali soltanto per lo svolgimento delle funzioni istituzionali. I dati personali raccolti (normalmente presso l'interessato) non possono eccedere le finalità per le quali sono stati raccolti i dati, come richiedere dati di familiari o affini quando queste informazioni non sono necessarie, ecc. il Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG), quale ente pubblico non economico non deve richiedere il consenso dell'interessato, salvo trattamenti diverse da quelli previste nelle normali funzioni istituzionali, come:

- Dati trasmessi ad altra scuola per trasferimento riguardante Fascicolo Personale (documenti anagrafici, documenti scolastici, ecc. o dati sensibili riguardanti lo stato di salute
- Trasmissione con strumenti cartacei o elettronici di dati di alunni riguardanti il curriculum o altri dati riguardanti la sfera personale, ad organizzazioni esterne (aziende, enti, ecc.)
- Certificati medici e altri dati sensibili o giudiziari trasmessi ad altri enti o scuole pubbliche per motivi di trasferimento
- La trasmissione con strumenti cartacei o elettronici di dati di collaboratori esterni riguardanti dati della sfera personale, ad organizzazioni esterne

L' Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG), quale ente pubblico non economico in riferimento ai **dati comuni**:

- È autorizzato da parte del Garante al trattamento di tutti i dati comuni, purché siano strettamente necessari all'attività istituzionale senza riferimento ad una norma di legge o un regolamento che lo preveda espressamente (art. 19).
- Presenta all'interessato l'informativa scritta o orale di cui all'art. 13, relativa al trattamento dei dati comuni. Per i dati comuni la firma per presa visione dell'informativa da parte dell'interessato non è obbligatoria, anche se l'Istituto stabilisce che la firma venga comunque apportata

- Può comunicare (il titolare sa chi riceverà i dati) mediante strumenti elettronici e non, dati comuni ad altri enti pubblici senza chiedere l'autorizzazione al Garante in quanto tale comunicazione è prevista espressamente da leggi e regolamenti. In caso di mancata norma, se la comunicazione è strettamente necessaria per lo svolgimento delle funzioni istituzionali, deve essere eseguita preventiva comunicazione al Garante (art. 39 e 181) che si riterrà autorizzata dopo 45 giorni sul principio del silenzio-assenso, salvo se il trattamento rientra in una delle Autorizzazioni generali (art. 40-41), pubblicate nella Gazzetta Ufficiale della Repubblica italiana. In tal caso il Titolare del trattamento non è tenuto a presentare al Garante una richiesta di autorizzazione se il trattamento che intende effettuare è conforme alle relative prescrizioni.
- Può diffondere (il titolare non sa a priori chi riceverà i dati) mediante strumenti elettronici e non, dati comuni senza chiedere l'autorizzazione al Garante se tale comunicazione sia prevista espressamente da una legge o regolamento. Esempi: esposizione all'albo o su Web di un documento

Di conseguenza valgono le seguenti regole:

- Ogni istanza rivolta alla scuola deve essere redatta su un modulo che in calce riporti per intero il testo dell'informativa relativa al trattamento dei dati comuni, in modo che la firma dell'istanza stessa funga anche da attestazione della presa visione dell'informativa stessa. Pertanto non si accettano istanze su fogli bianchi. Tassativamente vanno utilizzati gli appositi moduli che hanno la parte superiore bianca e in calce riportano l'informativa. In casi eccezionali l'informativa può essere applicata all'originale, però è necessaria coincidenza di data e un chiaro riferimento al documento a cui si riferisce
- Per quanto riguarda dipendenti, collaboratori, commissari d'esame ecc. al momento dell'inizio del rapporto l'informativa deve prevedere anche le probabili comunicazioni di dati personali alle varie istanze del MIUR, alla Regione, al Tesoro, alla Ragioneria Provinciale dello Stato, all'INPS (se T.D.) o all'INPDAP, al Ministero Funzione Pub-blica per l'anagrafe delle retribuzioni, alla scuola di provenienza e alla scuola a cui fossero trasferiti, ecc.
- Ai sensi dell'art. 48 del D. P. R. n. 445 del 28 dicembre 2000 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa), è obbligatorio inserire l'informativa nella modulistica per la presentazione delle dichiarazioni sostitutive di certificazione e di atto notorio.
- E' opportuno comunque inserire l'informativa in via generale in tutta la modulistica relativa alle istanze da presentare alla scuola.

L' Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG), quale ente pubblico non economico in riferimento ai **dati sensibili e giudiziari**:

- Può trattare i dati sensibili in quanto autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite (art. 20)
- Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, può trattare i dati sensibili "solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo"
- Se per il trattamento dei dati sensibili non è previsto espressamente da una disposizione di legge l'Istituto può "richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili", salvo se il trattamento rientra in una delle Autorizzazioni generali (art. 40-41), pubblicate nella Gazzetta Ufficiale della Repubblica italiana. In tal caso il Titolare del trattamento non è tenuto a presentare al Garante una richiesta di autorizzazione se il trat-tamento che intende effettuare è conforme alle relative prescrizioni.
- Può trattare dati giudiziari solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati

trattati e di operazioni eseguibili, fermo restando che non tutte le autorizzazioni del Garante sono date per finalità di rilevante interesse pubblico (solo quelle relative ai rapporti di lavoro e ai trattamenti sanitari) e diversamente dalle regole dei dati sensibili, non è prevista la comunicazione al Garante col meccanismo del silenzio-assenso dopo 45 giorni.

- Se per il trattamento dei dati giudiziari non è previsto espressamente da una disposizione di legge l'Istituto può "richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili", salvo se il trattamento rientra in una delle Autorizzazioni generali (art. 40-41), pubblicate nella Gazzetta Ufficiale della Repubblica italiana. In tal caso il Titolare del trattamento non è tenuto a presentare al Garante una richiesta di autorizzazione se il trat-tamento che intende effettuare è conforme alle relative prescrizioni
- Ai sensi dell'art. 22 c. 1 le modalità di trattamento devono essere volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'Interessato
- Ai sensi dell'art. 22 c. 2 nel fornire all'Interessato l'informativa (di cui all'articolo 13) fare espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari (può trattarsi di legge nazionale o regolamento o Provvedimento del Garante)
- Ai sensi dell'art. 22 c. 3 possono essere trattati solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa
- Ai sensi dell'art. 22 c. 4 i dati sensibili e giudiziari di regola devono essere raccolti presso l'Interessato
- Ai sensi dell'art. 22 c. 5 Il titolare deve verificare periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'Interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, il titolare valuta specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.
- Ai sensi dell'art. 22 c. 6, nel caso di dati gestiti con strumenti elettronici è necessario utilizzare tecniche di cifratura o sostituendo il nome dell'Interessato con un Codice identificativo o con altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.
- Ai sensi dell'art. 22 c. 7 nel caso di dati idonei a rivelare lo stato di salute e la vita sessuale conservare separatamente dagli altri dati personali trattati per finalità che non richiedono l'utilizzo dei predetti dati idonei ecc. e se trattati con strumenti elettronici alle modalità del punto precedente (cifratura o codici identificativi)
- Ai sensi dell'art. 22 c. 8 i dati sensibili e giudiziari non possono essere diffusi (il titolare non sa a priori chi riceverà i dati)
- Ai sensi dell'art. 22 c. 10 e 11 non utilizzare i dati nell'ambito di test psico attitudinali volti a definire il profilo o la personalità dell'Interessato Effettuare operazioni di raffronto tra dati sensibili e giudiziari oppure utilizzare i dati per definire il profilo o la personalità dell'Interessato, solo previa annotazione scritta dei motivi. Se queste operazioni o i trattamenti vengono effettuati utilizzando banche di dati di diversi titolari (= enti), sono ammessi solo se previsti da espressa disposizione di legge.

Di conseguenza valgono le seguenti regole:

- Ogni trattamento di dati personali sensibili o giudiziari deve prevedere la sottoscrizione per presa visione, da parte dell'interessato, dell'apposita informativa di cui all'art. 13, fornita dal Titolare., nella quale si dovrà fare espresso riferimento alla normativa che prevede gli obblighi o i compiti in

base alla quale è effettuato il trattamento dei dati sensibili e giudiziari (ciò non è obbligatorio nell'informativa relativa al trattamento dei dati comuni
- Ogni trattamento di dati personali (comuni, sensibili e giudiziari) deve essere tale da determinare il minimo sacrificio possibile del diritto alla riservatezza dell'Interessato (è illegittimo chiedere un dato in più di quello che è strettamente necessario)
- Ogni fase del trattamento deve rispettare le norme di legge e di regolamento
- Ogni fase di trattamento deve adottare le misure di sicurezza previste per la categoria alla quale il dato appartiene
- Ogni trattamento di dati personali sensibili o giudiziari deve rispettare i presupposti per avere la legittimazione a trattarlo
- In caso di comunicazione o diffusione, che il dato rientri nelle categorie autorizzate

Procedura PPD03: sottoscrizione dell'interessato e deleghe

Qualunque trattamento di dati su richiesta dell'Interessato, se presentato da terzi deve essere tassativamente autorizzato da delega. Ovviamente per gli alunni minorenni, il genitore o la persona esercente la potestà genitoriale non ha bisogno di delega. Per gli alunni maggiorenni anche il genitore ha bisogno della delega. La delega va allegata all'informativa o all'istanza o alla ricevuta.

Procedura PPD04: trasferimenti, abbandoni, cessazioni contratti, conclusione degli studi

I dati raccolti presso l'interessato alunno o dipendente che per vari motivi conclude i rapporti con l'istituto (trasferimenti conclusione degli studi, ecc.) vanno consegnati all'interessato stesso, salvo i documenti contenenti dati personali che la scuola è obbligata a conservare. Nel caso non fosse possibile trattare direttamente con l'Interessato, si deve mandare un avviso per il ritiro. Nel frattempo i materiali da consegnare vanno posti in busta chiusa. Al ritiro va fatta firmare una ricevuta. Se passato un lasso ragionevole di tempo, l'interessato un suo delegato non si presenterà a ritirarli, si avvierà una procedura di distruzione dei documenti, riportando tale operazione su un verbale ovviamente valutando prima se ci sono documenti che non sia opportuno eliminare (ad esempio, diplomi originali e simili). In ogni caso qualunque fascicolo personale che transiti dall'archivio corrente a quello storico, deve essere prima depurato di tutti dati personali non più necessari.

Quando l'alunno ha cessato al frequenza o il dipendente ha cessato di essere in carico alla scuola, il relativo fascicolo personale viene depurato dei documenti non più necessari, quindi archiviato nel corrispondente archivio storico, collocato in una stanza chiusa a chiave, ad accesso selezionato

Procedura PPD05: Regole generali per la sicurezza degli archivi

Gli archivi contenenti dati personali devono essere protetti dai seguenti eventi:

- Accesso da personale non autorizzato
- furto e manomissione dei dati
- distruzione o perdita dei dati dovuta ad eventi e fisici
- perdita accidentale dei dati per incuria o per distrazione.

Valgono le seguenti regole:

- I dati comuni sono conservati in appositi archivi (non necessariamente chiusi a chiave) ubicati in locali il cui accesso è consentito solo agli Incaricati del trattamento che osserveranno le procedure viste in precedenza
- I dati sensibili e giudiziari sono conservati in appositi archivi (armadi o cassettiere) dotati di serratura e chiusi a chiave la cui apertura è consentita solo agli Incaricati del trattamento che osserveranno le procedure viste in precedenza

- Gli archivi contenti dati personali devono essere funzionanti e muniti di idonea serratura a chiave. In caso di guasti è necessario segnalarli al responsabile di riferimento. In ogni caso l'Incaricato o il Responsabile devono verificare che gli elementi di arredo siano sempre chiusi e che vengano rispettate le misure relative alla gestione delle chiavi
- In caso di indisponibilità di arredi muniti di serratura per l'archiviazione dei documenti contenenti dati personali sensibili e giudiziari, gli archivi devono in ogni caso essere ubicati in appositi locali chiusi a chiave e, se appare agevole l'intrusione dall'esterno, muniti di sbarre. In tal caso il personale diverso dagli Incaricati del trattamento che vi accede deve essere accompagnato da uno dei soggetti Incaricati del trattamento o dal custode delle chiavi, che deve verificare che non avvenga un accesso illecito ai dati sensibili ivi contenuti
- Ogni ufficio contenente dati personali deve essere chiuso a chiave quando non presenziato, anche se i documenti sono custoditi in contenitori chiusi a chiave.
- Al fine di ridurre i rischi dovuti ad eventi fisici furti e manomissioni è opportuno:

  - Che gli archivi devono essere chiusi
  - Utilizzare le norme e i relativi dispositivi antincendio previsti dalle norme 81/08
  - L'impiego di un impianto antincendio con sensori e rilevazione di fumo
  - Controllare periodicamente la funzionalità dell'impianto antifurto
  - Controllare gli accessi del personale non autorizzato
  - Impiegare le procedure di conservazione dei dati come indicato ai punti precedenti
  - Gli armadi e contenitori che ospitano archivi vanno chiusi a chiave alla fine della giornata lavorativa e le chiavi vanno messe in luogo sicuro indicato dal DSGA.

Procedura PPD06: conservazione di registri e altri documenti utilizzati per anni scolastici precedenti e non più utilizzati

I documenti e i registri utilizzati solo per l'anno scolastico in corso sono conservati seguendo le procedure viste in precedenza. Dopo il trascorrere dell'anno scolastico non essendo più utilizzati, a meno di ricorsi o richieste di accesso legittime, vanno raggruppati riportando il contenuto e la scadenza per l'eliminazione. La conservazione avviene in archivio chiusa a chiave ad accesso selezionato. L'eliminazione dei documenti avviene mediante la procedura di distruzione dei documenti.

Procedura PPD07: scarto periodico dei documenti

Ai sensi dell'art. 11 c. e i dati personali oggetto di trattamento sono conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. Pertanto all'inizio di ogni anno è necessario controllare i documenti negli archivi e distruggere quelli non più necessari. L'eliminazione dei documenti avviene mediante la procedura di distruzione dei documenti.

Procedura PPD08: distruzione dei documenti

La distruzione di documenti contenenti dati personali di qualunque livello avverrà con modalità di Protezione Dati per impedire che estranei prendano visione del contenuto o, peggio, se ne impadroniscano. Di queste operazioni si occupano solamente Incaricati, con la qualifica di Collaboratori Scolastici e Assistenti Amministrativi. Se possibile si utilizza un apparecchio che trincia la carta. Altrimenti si provvede a rendere comunque anonimi mediante tagli e cancellature indelebili i documenti sensibili, giudiziari e particolari ad alto rischio. Per gli altri ci si assicurerà che nessuno possa impadronirsene prima della distruzione (o riciclo o conferimento in discarica) da parte dell'ente a cui si conferiranno.

Procedura PPD09: documenti provvisori

I dati personali contenuti in documenti provvisori quali appunti, bozze, stampe, fotocopie costituiscono elemento di rischio, maggiorato quando trattasi di pratiche comprendenti anche documenti sensibili o giudiziari. Pertanto essi vanno distrutti con la prescritta procedura o , se necessario conservarli, archiviati insieme all'originale del documento sensibile o giudiziario.

Procedura PPD10: fotocopiatura

Quando documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza devono essere fotocopiati, hanno la precedenza su tutti gli altri e devono essere adottate opportune cautele affinché nessun altro ne possa prendere visione. Tranne impossibilità tecnica, l'operazione di fotocopiatura deve essere effettuata dall'Incaricato che tratta la pratica. L'Incaricato deve fare in modo che il documento non venga lasciato in giacenza vicino alla fotocopiatrice né prima né dopo la fotocopiatura. A maggior ragione questo si applica se l'operazione di fotocopiatura avviene in una stanza ad accesso libero.

Procedura PPD11: utilizzo documenti da parte di terzi

Quando documenti contenenti dati personali di tipo sensibile, giudiziario o particolare ad alto livello di delicatezza devono essere movimentati attraverso collaboratori scolastici incaricati, anche all'interno della scuola, essi vanno collocati in busta chiusa. Anche la spedizione postale o la consegna in altro modo deve essere effettuata esclusivamente da incaricati che abbiano ricevuto almeno l'autorizzazione a questo ambito di trattamento e che assicurino massima diligenza nella custodia dei plichi.

Procedura PPD12: accesso in uffici da terzi (dati cartacei)

L'accesso agli uffici dove vengono effettuati trattamenti di dati personali sensibili e giudiziari, nelle ore lavorative, è riservato agli incaricati, al Dirigente, al DSGA e ai collaboratori scolastici che ne hanno motivo

L'accesso negli uffici dove sono presenti archivi contenenti dati personali da parte di dipendenti o estranei che hanno la necessità di accedere per motivi di pulizia, manutenzione o perché autorizzati su richiesta, deve essere effettuato solo con i contenitori chiusi a chiave. In alternativa tutte le operazioni devono essere effettuate in presenza di un incaricato della segreteria.

Gli uffici dove vengono effettuati trattamenti di dati personali sensibili e giudiziari devono essere chiusi a chiave quando non è presenziata dagli incaricati e dal personale autorizzato.

Istruzioni per la sicurezza mediante strumenti elettronici

Procedura PPD13: sistema di autenticazione e autorizzazione

Ai sensi dell'articolo 34 c. 1 del D.LGS. 196/03 il trattamento di dati personali con strumenti elettronici é consentito esclusivamente agli Incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Di conseguenza valgono le seguenti regole:

- Ogni incaricato sarà in possesso una credenziale di autenticazione elettronica individuale costituita da uno più nomi utente e password. La credenziale di autenticazione è prodotta dall'amministratore di sistema in quanto incaricato alla gestione dei sistemi informatici

- L'accesso ai dati avverrà mediante la credenziale di autenticazione individuale utilizzando il dispositivo di accesso indicato nella **Tabella 2.** In particolare la procedura di autenticazione avverrà a livello di sistema impostando la protezione della password mediante sistema operativo. Qualora questo non abbia tale funzione intrinseca occorre procedere alla protezione mediante password a livello di macchina (es. password impostata a livello di BIOS). I software di gestione dei dati personali (SISSI-SIDI), hanno un sistema di autenticazione intrinseco. Ciascun potrà accedere a questi sistemi utilizzando la credenziale di autenticazione personale affidata che potrà non coincidere con quella dell'elaboratore.
- Ogni incaricato deve adottare le necessarie cautele per assicurare la segretezza della credenziale di autenticazione
- La parola chiave deve essere 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. Essa non deve contenere riferimenti agevolmente riconducibili all'Incaricato (nomi o iniziali proprie o di parenti, date di nascita, e simili)
- La parola chiave deve essere modificata da ciascun incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi
- La generazione della parola chiave è a cura dell'amministratore di rete che provvederà a consegnarla all'incaricato. Tale consegna potrà avvenire utilizzando sistemi elettronici mediante un server di dominio al quale tutti gli elaboratori dovranno autenticarsi prima di avviarsi oppure utilizzando strumenti non elettronici mediante i quali la parola chiave sarà consegnerà personalmente o in busta chiusa se la consegna è indiretta. La parola chiave potrà essere modificata in seguito dall'incaricato cha la utilizzerà.
- Le parole chiave vanno conservate accuratamente da parte dell'incaricato. Sono ovviamente di facile individuazione le parole chiavi scritte in prossimità dell'elaboratore. Occorre utilizzare metodi di conservazione sicura come portare con sé il documento dove è conservata la parola chiave.
- La parola chiave è personale quindi non può essere assegnata ad altri incaricati, neppure in tempi diversi
- Le credenziali di autenticazione non utilizzate da almeno sei mesi vanno disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica
- L'incaricato di nuova assunzione o supplente avrà una nuova parola chiave. Essa sarà disattivata se il nuovo incaricato cessa il mandato.
- Le credenziali vanno disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali
- In caso di allontanamento dal dispositivo di accesso è necessario interdire la funzionalità mediante attivazione della maschera di richiesta delle credenziali di accesso. Comunque Gli incaricati non devono lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento
- Al fine di consentire al titolare la disponibilità dei dati o degli strumenti elettronici nei casi in cui si verifichi una prolungata assenza o impedimento dell'Incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, le parole chiave generate dall'amministratore di sistema ed eventualmente modificate dall'incaricato vanno consegnate al DSGA e all'amministratore di sistema in busta chiusa che la conserveranno in luogo sicuro. Tale procedura è automatica se è impiegato un server di dominio. In tal caso anche se la parola chiave non è conosciuta da nessuno è possibile crearne una nuova agevolmente. Queste procedure valgono anche nei casi di parole chiavi dimenticate oppure nuove parole chiavi da assegnare a figure nuove o sostitute dell'incaricato effettivo. Ovviamente le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione o all'uso personale o didattico
- Per problemi inerenti il buon funzionamento dei sistemi o per necessità di nuove configurazione contattare l'amministratore di sistema.

Nell'ambito del trattamento dei dati sensibili e giudiziari è necessario adottare un sistema di autorizzazione, inteso come l'insieme delle procedure tecniche tali da discriminare l'accesso a singoli incaricati a particolari classi o tipologie di dati negandolo al resto.

A tal proposito valgono le seguenti regole:

- I profili di autorizzazione sono implementabili nelle aree del software ARGO-SIDI In particolare gli incaricati accedono solo alle aree di propria competenze mediante funzioni di discriminazione degli accessi. In particolare ad ogni parola chiave del software ARGO-SIDI è associato un gruppo di aree di accesso
- Per quanto riguarda l'utilizzo di dati nei documenti creati con Microsoft Office non è previsto nessuna autorizzazione in quanto per motivi organizzativi e per agevolare il lavoro di gruppo ogni incaricato può accedere a questi tipi di dati.
- La gestione del sistema di autorizzazione è affidata all'amministratore di sistema

Procedura PPD14: sistema di cifratura dei dati idonei a rivelare lo stato di salute e la vita sessuale

Questa istituzione tratta dati idonei a rivelare lo stato di salute del personale, docente ed ATA e degli alunni esclusivamente per finalità previste dalla legge.

In riferimento all'art. 22 comma 7 del D.LGS. 196/2003 i dati idonei a rivelare lo stato di salute "sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo". I dati idonei a rivelare lo stato di salute, qualora contenuti in banche dati informatiche vengano trattati "con tecniche di cifratura o mediante l'utilizzo di codici identificativi o di altre soluzioni, che li rendono temporaneamente indecifrabili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità".

Allo stato attuale il Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG) generalmente tratta dati relativi allo stato di salute senza l'ausilio di strumenti elettronici. Tali dati consistono in certificati medici consegnati o fatti pervenire all'ufficio di segreteria amministrativa. Essi sono conservati nei fascicoli personale separati dagli altri documenti all'interno di appositi contenitori dotati di serratura. Dopo la ricezione, durante il trattamento, i dati saranno inseriti in un contenitore chiuso riferito all'interessato e successivamente inseriti nel fascicolo personale, dove saranno conservati all'interno di una busta chiusa recante l'indicazione del contenuto separatamente dagli altri documenti.

I dati relativi agli alunni sono essenzialmente certificati medici consegnati dagli alunni o dai genitori. Si tratta di documenti per giustificazione assenze, esonero da attività di educazione fisica, necessità di particolari diete alimentari, ecc.

Dopo la ricezione i dati saranno inseriti in un contenitore chiuso riferito all'interessato e successivamente trattati da personale incaricato e custoditi in appositi contenitori chiusi.

Qualora i dati idonei a rilevare lo stato di salute e la vita sessuale venissero trattati con strumenti elettronici quali documenti generati mediante Office, occorre memorizzare i file in cartelle separate da altri dati all'interno dello stesso elaboratore ovvero utilizzando all'occorrenza un server di dominio come descritto nella sezione 10.1. Tali dati dovranno impiegare un sistema di cifratura. Tale sistema è implementabile utilizzando uno dei seguenti suggerimenti:

- Utilizzare software di crittografia a chiave pubblica caratterizzato da algoritmi di ultima generazione (DSA, RSA, AES, 3DES, MD5, SHA-1, ecc.), firma digitale, distribuzione automatica amministrazione delle chiavi, configurato su ciascun elaboratore che tratti dati con obbligo di crittografia
- Utilizzare software di crittografia a chiave pubblica caratterizzato da algoritmi di ultima generazione (DSA, RSA, AES, 3DES, MD5, SHA-1, ecc.) .), firma digitale, distribuzione automatica amministrazione delle chiavi, configurato su un server in cui sono archiviati dati ai quali possono accedere utenti autorizzati

- Impiegare semplici sistemi di crittografia offerti dai sistemi operativi degli elaboratori, qualora questi ne siano provvisti.

Le chiavi di crittografia sono gestite in maniera protetta secondo le seguenti regole:

- Ogni incaricato sarà in possesso di una propria chiave di crittografia. La chiave può essere prodotta dall'amministratore di sistema in quanto incaricato alla gestione dei sistemi informatici oppure direttamente dall'interessato
- Ogni incaricato deve adottare le necessarie cautele per assicurare la segretezza della chiave
- La chiave deve essere di almeno 1024 bit
- La generazione della chiave è a cura dell'amministratore di rete che provvederà a consegnarla all'incaricato. Tale consegna potrà avvenire utilizzando sistemi elettronici mediante un server di dominio al quale tutti gli elaboratori dovranno autenticarsi prima di avviarsi oppure utilizzando strumenti non elettronici mediante i quali la parola chiave sarà consegnerà personalmente o in busta chiusa se la consegna è indiretta. La parola chiave potrà essere modificata in seguito dall'incaricato cha la utilizzerà.
- Le chiavi vanno conservate accuratamente da parte dell'incaricato.
- Al fine di consentire al titolare di assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'Incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, le chiavi generate dall'amministratore di sistema o dall'incaricato vanno consegnate al DSGA che le conserveranno in luogo sicuro. Tale procedura è automatica se è impiegato un server di dominio.
- Per problemi inerenti il buon funzionamento dei sistemi o per necessità di nuove configurazione contattare l'amministratore di sistema.

Procedura PPD15: protezione da accessi telematici dannosi

I dati personali devono essere protetti da accessi che possono compromettere l'integrità e la disponibilità delle informazioni. Gli accessi non autorizzati possono avvenire secondo una dei seguenti eventi:

- Accessi esterni nascosti finalizzati a intercettare, acquisire, sottrarre dati utilizzando tecniche di intrusione in genere non rilevabili dall'utente finale
- Accessi esterni finalizzati a recare danno ai sistemi informatici o a bloccarne l'uso (attacchi DOS Denial Of Service)
- Accessi di utenti non autorizzati presenti nella rete interna finalizzati a intercettare, acquisire, sottrarre dati utilizzando tecniche di intrusione in genere non rilevabili dall'utente finale
- Accessi di utenti non autorizzati presenti nella rete interna finalizzati a recare danno ai sistemi informatici o a bloccarne l'uso
- Accessi non autorizzati conseguenti ad azioni dell'incaricato quali collegamenti a siti non affidabili, scaricamento software dannoso, posta elettronica dannosa

I metodi di protezione dei dati da accessi telematici dannosi possono ricondursi alle seguenti categorie:

- Impiego di strumenti e apparecchiature per il controllo e il blocco di accessi interni o esterni non autorizzati
- Impiego di strumenti e apparecchiature per la protezione da software dannosi

Allo stato attuale il Istituto Comprensivo Statale "PALMIERI - S.GIOVANNI BOSCO" - San Severo (FG) è dotato di un sistema di protezione. Pertanto per quanto riguarda la protezione da accessi interni ed esterni non autorizzati valgono le seguenti regole:

- Il sistema di protezione garantisce una protezione di tipo firewall fra l'esterno (Internet) e la rete locale
- Il sistema di protezione garantisce funzioni di rilevazione e prevenzione delle intrusioni esterne.

- Per la protezione di software dannoso che provocherebbe danni mediante virus, worm, trojan ecc. il sistema di protezione consente in tal senso una protezione dall'esterno (Internet), mentre occorre installare su ogni elaboratore un valido programma antivirus caratterizzato da funzioni di aggiornamento almeno settimanale con controllo degli allegati di posta elettronica.

Procedura PPD16: uso dei supporti rimovibili

I dati personali devono essere memorizzati di regola negli appositi archivi elettronici indicati nell'allegato 2. La memorizzazione di dati personali in supporti removibili (floppy, CD, DVD, cassette, ecc.) è possibile solo momentaneamente. In alternativa tali supporti devono essere conservati con le stesse regole viste per il backup dei dati. I supporti removibili contenenti dati personali devono essere resi inutilizzabili (cancellazione, distruzione, ecc.) subito dopo il loro impiego.

Procedura PPD17: accesso in uffici da terzi (dati elettronici)

L'accesso agli uffici dove vengono effettuati trattamenti elettronici di dati personali, nelle ore lavorative, è riservato agli incaricati, al Dirigente, al DSGA e ai collaboratori scolastici che ne hanno motivo.

L'accesso negli uffici, dove sono presenti strumenti elettronici contenenti dati personali, da parte di dipendenti o estranei che hanno la necessità di accedere per motivi di pulizia, manutenzione o perché autorizzati su richiesta, deve essere effettuato solo con gli elaboratori spenti o inibiti con parola chiave. In alternativa tutte le operazioni devono essere effettuate in presenza di un incaricato della segreteria. In caso di manutenzione hardware e software occorre prestare attenzione che il tecnico non acceda a dati personali a meno che non sia stato incaricato.

Gli uffici dove vengono effettuati trattamenti di dati personali sensibili e giudiziari devono essere chiusi a chiave quando non è presenziata dagli incaricati e dal personale autorizzato.

Trattamenti da parte dei docenti

Procedura PPD18: registri

I registri personali devono essere sempre custoditi in modo sicuro.

I registri di classe devono essere consultabili solo dagli alunni della classe interessata e si deve vigilare perché non vi siano accessi non autorizzati. I collaboratori scolastici sono Incaricati di riporli in luogo sicuro quando terminano le lezioni.

Il registro dei verbali del consiglio di classe e qualunque altro registro di verbali, affidato per la scrittura, la firma o la consultazione, deve essere mantenuto protetto da accessi non autorizzati e riconsegnato quanto prima al Dirigente o alla segreteria perché lo riponga in luogo sicuro.

Procedura PPD19: certificazioni mediche e informazioni sullo stato di salute degli alunni

I dati personali in grado di rivelare lo stato di salute sono classificati "sensibili" e quindi protetti dalla visione di terzi che non sia strettamente necessaria. Quindi eventuali certificati medici vanno visionati solo se necessario, e subito restituiti all'interessato affinché li consegni in segreteria. Questo vale in particolare per i certificati di esonero o limitazione presentati per educazione fisica; l'insegnante prenda nota dei limiti da osservare e faccia recapitare dall'interessato il certificato in segreteria. A volte l'insegnante ottiene informazioni su particolari, anche gravi, problemi di salute dell'alunno che possono presentarsi durante le lezioni, in alcuni casi con grave rischio per la vita dell'alunno (allergie con pericolo di grave shock anafilattico, asma grave con pericolo di soffocamento, diabete grave, epilessia, cardiopatie gravi, ecc.) o

imbarazzanti (disturbi di continenza, ecc.), messe a disposizione dai genitori o dall'interessato. Se l'informazione è orale l'insegnante è tenuto al riserbo. Se esiste qualche comunicazione scritta, trattasi di dato sensibile e va trattato con particolari cautele, chiedendo al Titolare o al DSGA come fare.

Anche informazioni su particolari diete seguite dall'alunno o per motivi di salute o per motivi religiosi sono da considerare dato sensibile, pertanto va rivelato soltanto nei casi strettamente necessari ed omettendone la ragione.

Nel caso di alunni portatori di handicap che incide sulla didattica, la visione e la detenzione della relativa documentazione per l'integrazione è un dato di massima sensibilità in quanto idoneo a rivelare lo stato di salute. Pertanto i documenti dovranno essere visti soltanto dai docenti e personale strettamente necessario, conservati con elevata cautela, poi consegnati in segreteria inserendoli in busta chiusa su cui sarà annotato il nome dell'interessato, descrizione del contenuto, data e l'annotazione "Da conservare separatamente in armadio sicuro". Al suo posto, insieme agli altri elaborati si metterà un foglio con l'annotazione del luogo di conservazione.

Procedura PPD20: elaborati contenenti notizie particolari o sensibili

Nel caso un elaborato consegnato alla scuola contenga dati personali o familiari particolari o sensibili, va custodito con cura e poi consegnato personalmente in segreteria mettendolo in busta chiusa su cui sarà annotato nome dell'interessato, descrizione del contenuto, data e l'annotazione "Da conservare separatamente in armadio sicuro". Al suo posto, insieme agli altri elaborati si metterà un foglio con l'annotazione del luogo di conservazione.

Procedura PPD21: gestione degli elenchi degli alunni

Gli elenchi di alunni contengono dati personali e possono essere consegnati a terzi, soprattutto privati, esclusivamente per attività istituzionali della scuola. Va comunque chiesta l'autorizzazione al Dirigente perché potrebbe costituire atto illegittimo. La trasmissione con strumenti cartacei o elettronici di dati di alunni riguardanti il curriculum o altri dati riguardanti la sfera personale, ad organizzazioni esterne (aziende, enti, ecc.), avviene solo su consenso dell'interessato o di chi ne fa le veci

Procedura PPD22: documenti scolastici contenenti dati personali

Qualunque documento scolastico che contenga dati personali va custodito in modo che nessun altro possa visionarlo, copiarlo o impadronirsene. Se non c'è motivo di detenerlo, va riconsegnato in segreteria per l'archiviazione.

Trattamenti da parte dei membri di organi collegiali (anche esterni alla scuola)

Procedura PPD23: documenti, verbali, atti e delibere degli O.C.

I documenti, i verbali, gli atti e le delibere prodotti dai membri degli organi collegiali che contengono dati personali anche sensibili e giudiziari devono essere trattati in modo da non eccedere le finalità del trattamento stesso. I documenti vanno conservati negli archivi indicati nell'allegato 2 oppure se cessa il motivo di trattamento vanno distrutti o archiviati a cura della segreteria. Eventuali documenti possono essere trattenuti dai membri per il tempo strettamente necessario al motivo istituzionale per cui il dato è stato acquisito e poi riconsegnato. Eventuali procedure di trattamenti che dovessero apparire non di stretta pertinenza degli Organi Collegiali vanno autorizzati dal Dirigente.

Trattamenti da parte dei Collaboratori Scolastici e del Personale Ausiliario

Procedura PPD24: documenti scolastici gestiti dai collaboratori scolastici e dal personale ausiliario

Qualunque documento scolastico che contenga dati personali va custodito in modo che nessun altro possa visionarlo, copiarlo o impadronirsene. Se non c'è motivo di detenerlo, va riconsegnato in segreteria per l'archiviazione.

Procedura PPD25: trasporto di documenti scolastici

I documenti ricevuti aperti vanno immediatamente consegnati alla segreteria, senza prenderne visione. Se c'è il sospetto che si tratti di certificati medici, certificazioni relativi ai redditi, ecc. l'interessato deve conservarli in busta chiusa.

I documenti destinati alla corrispondenza (sia in entrata, sia in uscita) vanno trattati con cura, protetti da accesso di terzi, mai lasciati incustoditi, consegnati appena possibile alla segreteria o al legittimo destinatario.

Nel caso di documenti da consegnare internamente alla scuola vanno adottate analoghe cautele.

Procedura PPD26: custodia uffici

Le stanze contenenti archivi e non presenziate devono essere mantenute chiuse controllando l'accese di personale no autorizzato. Le chiavi degli uffici dove avvengono trattamenti di dati personali sono a cura del DSGA L'ufficio del Dirigente Scolastico e gli uffici amministrativi in genere vanno chiusi a chiave quando non presenziati dal relativo personale.

E' fatto divieto assoluto a chiunque non ne abbia ricevuto esplicita autorizzazione di accendere o utilizzare gli elaboratori degli uffici amministrativi e del Dirigente Scolastico o che comunque contengano dati personali. Si deve intervenire immediatamente se una persona non autorizzata tenta di farlo.

Fuori dall'orario di apertura della scuola non si deve far entrare nei locali citati alcun estraneo.