D.P.S.

Azienda	*Ministero dell' Istruzione, dell'Università e della Ricerca* UFFICIO SCOLASTICO REGIONALE PER LA SICILIA **ISTITUTO COMPRENSIVO STATALE** **"Garibaldi-Capuana"** Via Porta Palermo, 223 – Raffadali

DOCUMENTO PRIVACY SCUOLE (D.P.S.) Aggiornato al regolamento UE 679/2016 (GDPR)

Dirigente scolastico:
Dott. Silvana Spirio

Responsabile del trattamento dati:
Ins. Gerlando Alonge

Data, 24/05/2018

Organigramma 2017-18
Dirigente Scolastico
Dott. Silvana Spirio

COLLABORATORI

- Alonge Gerlando (vicario)
- La Porta Rossana
- Vizzì Salvina
- Capraro Michela

DSGA

Vincenza Faseli

RESPONSABILI DI PLESSO

Scuola dell'Infanzia "Garibaldi " - Raffadali: INS. PACI PINA

Scuola dell'Infanzia e Primaria "Plesso Nuovo" – Santa Elisabetta: INS. MICCICHÈ ROSALIA

Scuola Secondaria di I Grado "Capuana" - SantaElisabetta: PROF.SSA PENDOLINO MARIA LUISA

FUNZIONI STRUMENTALI AL PTOF

COGNOME E NOME DEL DOCENTE	*AREA FUNZIONE STRUMENTALE*	*DESCRIZIONE*
➢ **Alonge Gerlando** ➢ **La Porta Rossana**	Area 1	Gestione PTOF
➢ **Vizzì Salvina** ➢ **Alaimo Maria Antonietta R.**	Area 2	Informatica e nuove tecnologie
➢ **Sicilia Giovanna (Raffadali)** ➢ **Lana Antonia M. (S. Elisabetta)**	Area 3	Interventi e servizi per gli studenti – Supporto al lavoro dei docenti
➢ **Iacono Manno Calogero** ➢ **Pendolino Maria L.**	Area 4	Disagio, integrazione e alunni diversamente abili
➢ **Mangione Antonina** ➢ **Bartolomeo Gerlanda**	Area 5	Autodiagnosi e autovalutazione d'Istituto

IL REGOLAMENTO UE 679/2016

Il Regolamento *Europeo 679 del 2016* è entrato in vigore il 24 maggio 2016 ed, essendo un atto "self-executing" è immediatamente esecutivo nell'ordinamento degli Stati membri (art. 288TFUE); tuttavia per espressa previsione normativa sostituirà la disciplina previgente *a partire dal 25 maggio 2018* (considerando 171 e art. 99, Reg. UE n. 2016/679).

Gli Stati membri hanno avuto, pertanto, a disposizione un considerevole lasso di tempo per l'aggiornamento della disciplina interna.

Il Regolamento introduce nuovi istituti, come il diritto all'oblio e alla portabilità dei dati, e stabilisce inoltre anche criteri volti a responsabilizzare imprese ed enti in materia di protezione dei dati personali e introduce agevolazioni per chi si conforma alle *regole di tutela dei dati*.

Le norme così introdotte hanno il compito di sostituire la precedente legislazione degli anni Novanta dello scorso secolo (la Direttiva 95/46, la cosiddetta Direttiva Madre), divenuta obsoleta anche in ragione dell'introduzione di tecnologie all'epoca inesistenti.

Il recente Regolamento Europeo 679 del 2016 prende atto delle nuove sfide per la protezione dei dati che l'evoluzione tecnologica e la globalizzazione comportano, oltre a considerare che la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo.

Le recenti iniziative legislative in materia di protezione dei dati mirano ad adeguare la normativa ai mutamenti dettati dall'evoluzione tecnologica soprattutto in tema di un aumento dei flussi transfrontalieri e dei dati scambiati tra pubblici e privati.

Pertanto, il legislatore europeo sottolinea come tale evoluzione tecnologica richieda un quadro normativo più solido e coerente in materia di protezione dei dati nell'Unione il quale, affiancato da efficaci misure di attuazione, contribuisce a creare il clima di fiducia necessario per lo sviluppo dell'economia digitale in tutto il mercato interno.

Il Regolamento UE 2016/679 non contiene una normativa differenziata in ragione dello status di titolare del trattamento pubblico o privato e non contiene neanche norme specificamente dedicate al settore pubblico. Alcune attività riguardano, tuttavia, solo lo svolgimento di attività pubbliche. Alla base della normativa non vi è, dunque, la natura pubblica o privata del titolare del trattamento ma la tipologia del trattamento stesso. Di

conseguenza, l'intero provvedimento è suscettibile di essere applicato alla Pubblica Amministrazione.

Il Regolamento sulla protezione dei dati personali n. 679 del 2016, pienamente applicabile dal 25 maggio 2018, predispone una disciplina unitaria del trattamento dei dati rispondente alle attese del processo globale di digitalizzazione, e contestualmente rappresenta l'introduzione di una impostazione innovativa in materia di privacy. La normativa, infatti, introduce importanti principi tra cui quello di *"accountability" (responsabilizzazione)*.

L'*accountability* costituisce una notevole sfida per le pubbliche amministrazioni, poiché richiede un significativo cambio di approccio, teso a modificare i ruoli del titolare del trattamento

dei dati e dell'interessato. In applicazione di tale principio spetta, dunque, al titolare del trattamento provare il rispetto delle regole in materia di trattamento dei dati, e contestualmente adattarsi ai nuovi istituti di Valutazione di impatto privacy, o notificazione delle violazioni o ancora di idoneità delle misure di sicurezza, con l'obiettivo comune di assegnare massima trasparenza all'agire amministrativo.

A titolo esemplificativo, il Regolamento statuisce che quando la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative. È evidente, dunque, che i soggetti pubblici, e pertanto anche le scuole dovranno far ricorso ad esperti competenti nella gestione dei dati, affinché realizzino le valutazioni necessarie in materia. A ciò si aggiunga che è inoltre stata prevista la figura obbligatoria del Data Protection Officer e, pertanto, la nuova regolamentazione impone alle amministrazioni, e dunque anche alle scuole, nuovi adempimenti e numerose attività di adeguamento.

SCOPO E AMBITO DI APPLICAZIONE DEL DPS

Il presente Documento sulla Privacy della Scuola (definito anche DPS) è adottato, ai sensi delle nuove disposizioni dettate dal nuovo regolamento europeo sulla Privacy 679/2016 e dell'art. 34 del Decreto Legislativo n. 196 del 30 giugno 2003 e relativo allegato B, per definire le politiche di sicurezza in materia di trattamento di dati personali nonché i criteri tecnico-organizzativi per la loro attuazione. Il documento, inoltre, fornisce idonee informazioni relative alla tipologia

di dati sensibili trattati secondo quanto previsto dagli articoli 20 comma 2 e 21 comma 2 del citato Decreto Legislativo e all'analisi dei rischi connessi all'utilizzo degli strumenti mediante i quali viene effettuato il trattamento.

Gli allegati al presente documento costituiscono parte integrante del Documento Programmatico Sulla Sicurezza dei dati.

Nel presente documento e nei relativi allegati i termini Trattamento, Dato personale, Dati identificativi, Dati sensibili, Dati giudiziari, Titolare, Responsabile, Incaricato, Interessato, Diffusione, Banca dati e tutti gli altri termini sono usati in conformità alle definizioni elencate nel Regolamento UE 679/2016. In dettaglio il Documento Programmatico Sulla Sicurezza fornisce informazioni relative a:

- l'elenco dei trattamenti di dati personali;
- indicazione del trattamento dei dati sensibili e giudiziari e descrizione riassuntiva del contesto in conformità al parere espresso dal Garante, ai sensi dell'art. 154, comma 1, lettera g) de! citato Decreto Legislativo.
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati.
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento garantendone la disponibilità in tempi certi compatibili con i diritti degli interessati;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità ai codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare *per* la cifratura o *per* la separazione di tali dati dagli altri dati personali dell'interessato.

di ogni anno, sarà oggetto di opportune revisioni per adeguarlo ad eventuali modifiche normative, al mutato livello di rischio a cui sono soggetti i dati trattati, ad eventuali assegnazioni o revoche di incarichi, all'utilizzo di nuovi strumenti informatici o in generale a un mutato assetto organizzativo.

Il GDPR e l'approccio adottato

Il Nuovo regolamento UE 679/2016 e il Codice sulla privacy - Decreto legislativo n° 196 del 30-6-2003) e il Decreto 7.12.2006 n. 305 impongono di rispettare alcuni principi fondamentali a **garanzia della riservatezza dei dati personali.**

Il presente DPS è stato redatto a seguito di una rilevazione sistematica dei dati personali trattati dall' Istituzione scolastica e di un'analisi dell'infrastruttura tecnologica esistente, con particolare riferimento alle caratteristiche della rete, dei Personal computer, dei sistemi di sicurezza in uso.

E' seguita un'analisi dei rischi ed una valutazione in ordine alla possibilità che possano verificarsi episodi di utilizzo improprio dei dati, di loro perdita o distruzione e di accesso non autorizzato.

Sono state, di conseguenza, definite misure ulteriori, rispetto a quelle già in essere, per ridurre i rischi rilevati.

I trattamenti sono legati alla erogazione dei servizi formativi ed educativi della istituzione scolastica, ai connessi rapporti con gli alunni e le famiglie, agli adempimenti relativi alla gestione e alla formazione del personale, agli adempimenti di contabilità e bilancio.

In linea generale, i dati trattati riguardano:

- persone fisiche, identificate o identificabili, quali nominativo, data di nascita, residenza, domicilio, stato di famiglia, codice fiscale, obblighi di leva, convinzioni religiose, filosofiche, politiche, vita sessuale, stato di salute, dati sindacali;
- persone giuridiche quali la forma giuridica, la sede legale, la data di costituzione, informazioni relative agli organi rappresentativi e legali, partita Iva, codice fiscale, la titolarità di diritti o la disponibilità di beni strumentali;
- presenze, prestazioni previdenziali, stipendi, permessi, ferie, malattia, stato di servizio e altri dati connessi al rapporti di lavoro del personale della scuola;
- procedimenti di natura penale, civile, tributaria e amministrativa;
- rapporti del dirigente scolastico e dei docenti con le famiglie;
- attività degli organi collegiali dell'istituzione scolastica;
- atti negoziali od offerte commerciali provenienti da fornitori di beni e servizi, ivi comprese eventuali attività professionali svolte a fini formativi;
- rapporti e convenzioni con aziende e agenzie formative, per stage e tirocini degli

alunni;

- altri soggetti, situazioni, eventi in applicazione di disposizioni di Legge o Regolamenti.

Revisione 2018 – Documento Privacy Scuola

aggiornato al GDPR n° 679/2016

- **Visto** Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito *RGPD*), in vigore dal 24 maggio 2016, e applicabile a partire dal 25 maggio 2018

- **Visto** il D. Lgs. 30 giugno 2003, n. 196 - "Codice in materia di protezione di dati personali" (in seguito semplicemente "Codice");

- **Considerato** che l'Istituzione Scolastica **Istituto Comprensivo Statale "Garibaldi-Capuana",** con sede a Raffadali in via Porta Palermo, 223, in quanto dotata di un autonomo potere decisionale, ai sensi dell'art.28 del d.lgs. n. 196 del 2004, deve ritenersi titolare del trattamento di dati personali;

- **Atteso** che la suddetta Istituzione Scolastica è tenuta a prevedere ed applicare le misure minime di sicurezza di cui agli artt. 31 e ss. del D. Lgs. n. 196/2003 nonché le nuove misure minime ICT Ai sensi della Direttiva PCM del 01/08/2015 e della CIRCOLARE 18 aprile 2017 , n. 2/2017;

- **Visto** il D. Lgs. 7 dicembre 2006, n. 305 - "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli artt. 20 e 21 del D. Lgs. n. 196/2003;

- **Visto** quanto previsto dall"art.45 del D.L. n.5 del 9 febbraio 2012 (c.d. Decreto „Semplifica Italia"), convertito nella L. n. 35 del 4 aprile 2012;

- **Valutata** la necessità di predisporre ugualmente un Documento interno che attesti il rispetto da parte dell' Istituzione Scolastica di quanto stabilito dal Codice e dal GDPR;

il seguente Documento valido per l'a.s. 2017/18 e per l'anno scolastico 2018/19.

Scopo del presente Documento è quello di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logistiche, secondo la descrizione e gli opportuni allegati, che fanno parte integrante del Documento, che saranno adottate da questa Istituzione Scolastica relativamente al trattamento dei dati personali, per le rispettive competenze, da parte del Direttore S.G.A., degli Assistenti Amministrativi, del Personale Docente e dei Collaboratori Scolastici.

Il Documento contiene idonee informazioni riguardo:

1. l'elenco dei trattamenti di dati personali;
2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
3. l'analisi dei rischi che incombono sui dati;
4. 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;
5. la previsione di interventi formativi degli INCARICATI del trattamento;
6. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del TITOLARE.

FINALITA' E SCOPI

Il presente documento, elaborato al fine di mettere in atto le misure di cui al regolamento UE 679/2016, per tutelare i dati personali oggetto di trattamento, si propone di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato da tutto il personale della **Istituto Comprensivo Statale "Garibaldi-capuana",** con sede a Raffadali in Via Porta Palermo 223, il cui rappresentante pro-tempore è il Dirigente Scolastico **Dott. Silvana Spirio** che nel seguito del documento sarà indicato come "**titolare**".

I provvedimenti organizzativi disposti e le misure di sicurezza adottate in osservanza a quanto disposto dal predetto regolamento sono finalizzati a garantire a ciascun "**interessato**" (utente, dipendente, fornitore) la tutela di:

- rispetto della privacy, della riservatezza dei dati, della tutela della dignità personale, dell'identità personale;
- rispetto della riservatezza, con riguardo alla tutela dei dati personali, anche allo scopo di evitare l'ingerenza di terzi;
- riservatezza delle documentazioni custodite dalla scuola e salvaguardia dell'integrità nel tempo delle documentazioni medesime, siano esse costituite da materiale cartaceo, che registrate su supporti informatici.

RIFERIMENTI NORMATIVI

- Legge 31/12/1996 n. 675 e successive modifiche;
- Legge 31/12/1996 n. 676, *recante delega al governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;*

- DPR 28/07/1999, n. 318 – *Regolamento recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali;*
- Legge 24/03/2001 n. 127, *recante delega la governo per l'emanazione di un T. U. in materia di trattamento dei dati personali;*
- Decreto legislativo 30/06/2003 n. 196 – *Codice in materia di protezione dei dati personali, in particolare:*

    - degli articoli da 28 a 30 (Soggetti che effettuano il trattamento);
    - degli articoli dal 31 al 36 (Misure di sicurezza);
    - degli articoli 59 e 60 (Disposizioni relative a specifici settori – Trattamento in ambito pubblico);
    - degli articoli 95 e 96 (Disposizioni relative a specifici settori – Istruzione);
    - dell'articolo 180 (Disposizioni transitorie – Misure di sicurezza);
    - dell'allegato B (Disciplinare tecnico in materia di misure minime di sicurezza).

- *Decreto Ministeriale n° 305 del 07/12/2006, regolamento dati sensibili e giudiziari trattati dal Ministero P.I.;*
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *«relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)»* (di seguito *RGPD*),

ADEGUAMENTO AL REGOLAMENTO DEI DATI SENSIBILI E GIUDIZIARI EMANATO DAL MIUR

Il presente D.P.S. è aggiornato alle novità introdotte dal **D.M. del Ministro della Pubblica Istruzione 7 dicembre 2006, n. 305**, pubblicato sulla G.U. n. 11 del 15 gennaio 2007: "*Regolamento recante l'identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali»"* (d'ora in poi "Regolamento").

Il Regolamento innova la disciplina sul trattamento dei dati sensibili e giudiziari nelle scuole, circoscrivendo i casi in cui è possibile trattare tali dati e specificando le operazioni su di essi eseguibili. In particolare:

- non è consentito il trattamento dei dati sensibili e giudiziari se non per finalità di rilevante interesse pubblico individuate dalla legge e specificate nel Regolamento;
- non è consentito il trattamento dei dati sensibili e giudiziari se non nell'ambito dei processi\procedimenti individuati nel Regolamento;
- i dati sensibili e giudiziari non previsti dal Regolamento non possono essere utilizzati e trattati;
- non è possibile comunicare dati sensibili e giudiziari a enti pubblici o privati se non nei casi previsti dal Regolamento.

ARTICOLAZIONE DEL DOCUMENTO

Conformemente a quanto prescrive il nuovo regolamento UE 679/2016 e dal punto 19 del "disciplinare tecnico allegato sub b) al d.Lgs. 196/2003, nel presente documento sono evidenziati:

1. i dati personali trattati;
2. l'indicazione delle sedi e la descrizione dei locali e degli strumenti con i quali si effettuano i trattamenti;
3. il titolare del trattamento dei dati;
4. la distribuzione dei compiti e delle responsabilità;
5. l'analisi dei rischi che incombono sui dati;
6. le misure minime ICT adottate e da adottare per garantire l'integrità e la disponibilità dei dati;
7. i criteri per l'adozione delle misure minime di sicurezza dei dati;
8. i criteri per la formazione del personale;
9. le dichiarazioni di impegno.

DEFINIZIONI

S' intende per:

1) **«dato personale»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) **«trattamento»**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la struttu- razione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) **«profilazione»**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) **«pseudonimizzazione»**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) **«archivio»**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) **«titolare del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o

degli Stati membri;

8) **«responsabile del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) **«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comuni- cazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comuni- cazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) **«terzo»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) **«consenso dell'interessato»**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'inte- ressato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) **«violazione dei dati personali»**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) **«dati genetici»**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico

della persona fisica in questione;

14) **«dati biometrici»**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

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

16) **«stabilimento principale»**:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'ammini- strazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) **«rappresentante»**: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente

regolamento;

18) **«impresa»**: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) **«gruppo imprenditoriale»**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) **«norme vincolanti d'impresa»**: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) **«autorità di controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) **«autorità di controllo interessata»**: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo;

23) **«trattamento transfrontaliero»**:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

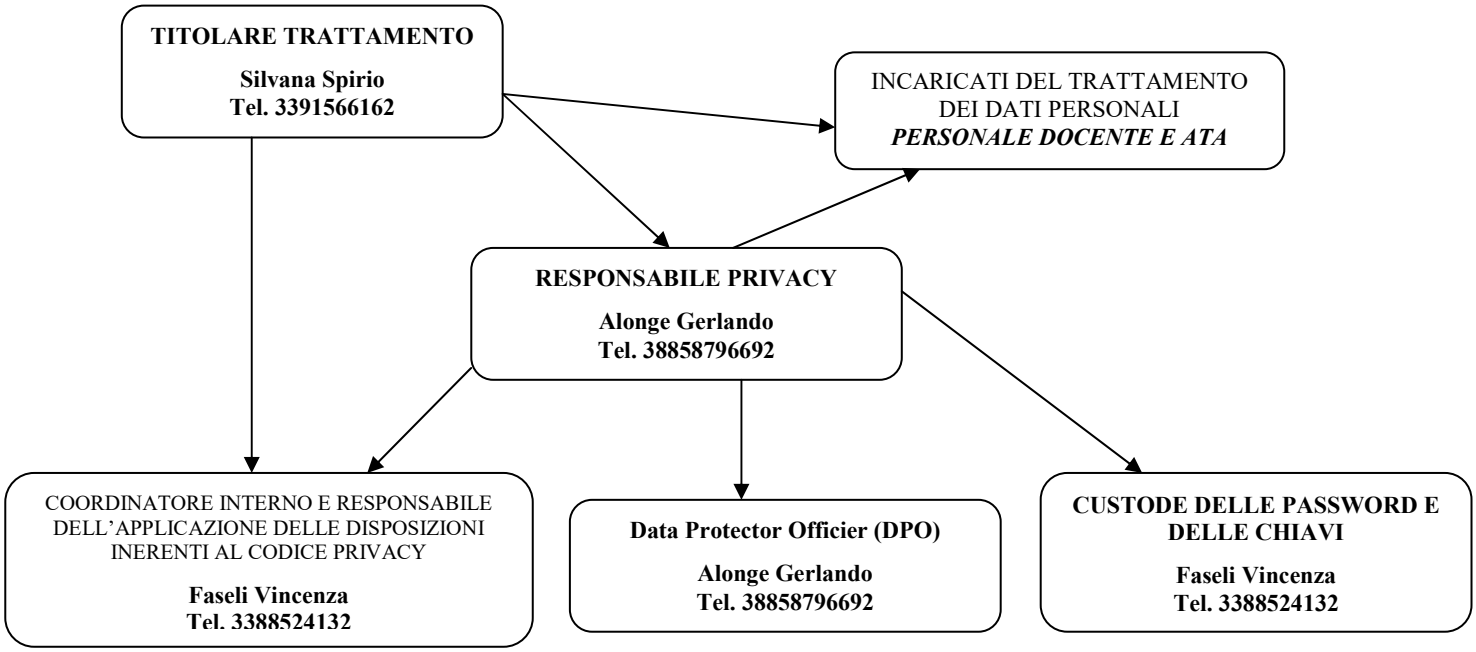
b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) **«obiezione pertinente e motivata»**: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) **«servizio della società dell'informazione»**: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ([1]);

26) **«organizzazione internazionale»**: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

ORGANIGRAMMA DELLE MANSIONI E RESPONSABILITA'



RESPONSABILITÀ

I responsabili, gli incaricati del trattamento e i manutentori del sistema sono individuati con apposito provvedimento che specifica finalità e modalità del trattamento autorizzate.

Titolare del trattamento

Titolare del trattamento è l' Istituzione Scolastica, con sede in Via Porta Palermo, 223 a Raffadali (AG) nella veste del suo rappresentante legale pro-tempore, il Dirigente Scolastico.

Il Dirigente Scolastico in qualità di titolare del trattamento dei dati

- è responsabile dell'analisi e della valutazione dei rischi ai fini dell'adozione di misure di sicurezza, sia idonee che minime;

- procede alla predisposizione delle misure idonee ritenute indispensabili nella struttura, valuta la congruità tecnico-economica delle misure proposte e quindi disporre l'adozione delle stesse;
- individua il/i responsabile/i del trattamento e con apposito incarico ne stabilisce le responsabilità in merito al rispetto degli adempimenti e delle prescrizioni stabiliti sulla base del D.Lgs196/03;
- si avvale della collaborazione del D.S.G.A. e dei responsabili dei diversi settori per la definizione della modulistica e delle procedure.

Responsabile del trattamento

Al responsabile del trattamento sono attribuiti incarichi di ordine organizzativo e direttivo, ed egli provvede a:
- individuare e designare per iscritto gli incaricati del trattamento che operano sotto la sua diretta autorità indicando
puntualmente l'ambito del trattamento consentito;
- impartire loro specifiche istruzioni scritte relative alle modalità di trattamento ammesse;
- organizzare la formazione per gli incaricati;
- procedere alle verifiche specificate nell'incarico.

E' stato individuato quale Responsabile del trattamento dei dati comuni e sensibili l'ins. Gerlando Alonge (Docente interno).

D.P.O (Data Protector officer)

Il Titolare del trattamento conferisce l'incarico di Responsabile della protezione dei dati personali (DPO) che assume i seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
b) sorvegliare l'osservanza del RGPD, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del RGPD;
d) cooperare con il Garante per la protezione dei dati personali;
e) fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

Incaricati del trattamento

L'assegnazione del personale docente e ATA alla specifica unità operativa, per la quale è individuato con atto formale, comporta l'automatico incarico al trattamento autorizzato per iscritto agli addetti all'unità medesima e la consegna, a cura del Responsabile del Trattamento, delle specifiche istruzioni scritte relative alle modalità di trattamento ammesse.

Per il personale amministrativo la designazione per iscritto riguarda un singolo incaricato e con essa si individua l'ambito del trattamento a questi consentito.

Di norma tali incarichi sono assegnati a partire dal I settembre, data di inizio del nuovo anno scolastico che coincide con le assegnazioni di sede del personale.

Sia per i trattamenti effettuati con strumenti elettronici, che per quelli che avvengono senza l'ausilio di tali strumenti, l'autorizzazione al trattamento è soggetta ad aggiornamento periodico e comunque almeno annuale, quando viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione riguardo l'ambito di trattamento consentito sia ai singoli incaricati che agli addetti alla manutenzione e gestione degli strumenti elettronici

DATI E BANCHE DATI

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare:

- sono precisate le finalità del trattamento;
- sono individuati i tipi di dati personali trattati, in base alla loro natura (comuni, giudiziari o sensibili ed alla categoria di soggetti cui essi si riferiscono (alunni, personale dipendente, fornitori, …..)
- sono definite le operazioni di trattamento dei dati effettuate;
- sono descritte le aree, i locali e gli strumenti con i quali si effettuano i trattamenti.

Finalità del trattamento

Al fine di perseguire le finalità istituzionali, l'Istituto effettua operazioni di trattamento di dati personali (sia comuni che sensibili o giudiziari) di studenti, personale dipendente, fornitori con le seguenti finalità:

a. la selezione e il reclutamento del personale a tempo determinato, nonché l'instaurazione, la gestione e la cessazione del rapporto di lavoro;

b. la frequenza dei corsi di studio;

c. l'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami;

d. l'attivazione degli organismi collegiali e delle commissioni istituzionali previsti dall'ordinamento scolastico;

e. l'acquisizione di beni, servizi e opere;

f. la difesa in giudizio del Ministero dell'istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrative, nonché quelle connesse alla gestione degli affari penali e civili;

g. le attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, etc.) con gli alunni e con le famiglie, e tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche.

DOCUMENTAZIONI

1. dati personali relativi agli alunni (registri di classe contenenti i recapiti delle famiglie e comunicazioni varie, con esclusione di ogni documentazione che possa contenere dati "sensibili");
2. dati personali sensibili relativi agli alunni (certificazioni mediche, certificazioni di deficit, diagnosi, ecc..) ;

3. dati sensibili relativi ai genitori degli alunni (istanze contenenti dati relativi alla situazione patrimoniale, documentazioni giudiziarie, documentazioni mediche prodotte a corredo delle domande di iscrizione o di altre domande)
4. dati personali relativi ai dipendenti;
5. dati personali sensibili relativi ai dipendenti;
6. dati personali riservati, relativi ad alunni, genitori e personale dipendente,
7. riguardanti corrispondenza riservata custodita dal dirigente, compresi gli atti relativi ai provvedimenti disciplinari;
8. dati personali relativi ai fornitori;
9. dati personali di anni precedenti, sistemati in archivio; **sono escluse le documentazioni contenenti dati sensibili.**

Struttura dell'edificio in cui sono custoditi i dati personali:

Il sito è circondato da una protezione perimetrale con cancelli d'accesso che sono sorvegliati durante le ore di attività e chiusi a fine giornata lavorativa. Inoltre, l'edificio è circondato su tutti i lati da fari illuminanti nel periodo notturno. Dispone, inoltre, di fari anche per l'illuminazione di lati o cortili interni. La sede non è difesa nelle porte d'accesso e nelle finestrature con vetri antisfondamento o inferriate. L'edificio di recente costruzione si presenta efficiente sia per quanto concerne gli impianti tecnologici che relativamente alla struttura architettonica interna.
I locali dove vengono trattati dati personali, sia per mezzo di documenti cartacei che attraverso applicazioni ed archivi informatici, sono situati all'interno dell'area dedicata agli uffici di segreteria il cui accesso è sempre presidiato durante il normale svolgimento dell'attività lavorativa.

Misure di sicurezza (TU81/2008)

Il sistema antincendio è costituito da estintori manuali a polvere ed anidride carbonica omologati. E' garantita la manutenzione con controllo d'efficienza semestrale da parte di

una società specializzata e si provvede ad assicurare la continuità nell'addestramento di personale preposto sull'uso degli estintori stessi.
La sede non è provvista di rilevatori di fumo. È stato predisposto un piano d'evacuazione, sono ubicati nei punti necessari e visibili al pubblico le procedure scritte da seguire in caso d'emergenza, è funzionante l'impianto d'illuminazione d'emergenza nei locali d'accesso al pubblico.
L'impianto elettrico è a norma. È presente per le postazioni di lavoro e il server un sistema d'alimentazione, specifico, dedicato, separato dagli altri contesti utilizzatori e con potenza adeguata, che soddisfa la necessaria continuità elettrica di funzionamento.

INFORMAZIONI SULLA TIPOLOGIA DEI DOCUMENTI E SUGLI STRUMENTI

Sia in forma cartacea che informatizzata, nei predetti uffici sono trattati documentazioni complete riguardanti gli alunni, relativi al corso di studi, alla presenza di handicap, alla certificazione dell'idoneità alla pratica sportiva non agonistica, alla scelta dell'insegnamento della religione cattolica. Documenti prodotti dalle famiglie, riguardanti la certificazione della situazione patrimoniale. Tutta la documentazione riguardante i docenti e il personale ATA, con elementi di individuazione di appartenenza sindacale, stato di salute, anche di congiunti per i quali vengono richiesti benefici previsti da particolari norme, allo stato di servizio, alla retribuzione, alle eventuali pratiche disciplinari e giudiziarie.

STRUTTURA DEL DOCUMENTO

Nell'impostare la struttura del documento si è tenuto conto degli esempi pubblicati nel sito web del Garante, nonché della "Guida operativa per redigere il documento programmatico"

Vengono, pertanto, fornite le seguenti "Informazioni essenziali":

Indicazione della finalità perseguita e dell'attività svolta dall'Istituzione scolastica:

- Garanzia del servizio scolastico offerto all'utenza
- Gestione del personale interno con contratto a tempo determinato e indeterminato
- Certificazione degli esiti scolastici e dei servizi prestati dai dipendenti
- Acquisizione di beni e servizi da terzi fornitori

Natura dei dati trattati:

Dati personali di alunni, genitori e dipendenti, tra i quali, assimilabili alla connotazione di "dati sensibili", vengono indicati quelli relativi alla presenza di certificazione della situazione di handicap relativa ad alcuni alunni, alla casuale presentazione di documentazioni prodotte da dipendenti o utenti, recanti notizie sullo stato di salute dei soggetti interessati.

Luoghi di tenuta e trattamento dei dati

I dati su supporto cartaceo e i dati acquisiti attraverso il protocollo riservato, sono conservati presso la Sede Centrale dell'Istituzione Scolastica.
I dati su supporto elettronico sono conservati negli archivi elettronici:

- dei computer dei servizi amministrativi ;
- nel *server* di Istituto.

I Servizi strumentali, concernenti l'assistenza e la manutenzione degli strumenti elettronici (elaboratori e programmi), sono affidati all'esterno,

Banca dati:

Tutti i dati contenuti in documentazione cartacea vengono raccolti e conservati negli armadi degli uffici di segreteria e nell'archivio. I dati relativi al personale, agli alunni ed alla gestione economico-contabile, anche con riferimento all'identità dei fornitori, sono trattati mediante elaborazione elettronica costituita da software acquisiti dalla ditta **Argo-Software**

Tipologia di accesso:

L'accesso agli uffici è consentito solo al personale addetto specificamente incaricato.

Tutti i computer presenti negli Uffici sono bloccati da password di cui sono a conoscenza esclusivamente gli addetti incaricati.

Tipologia di interconnessione:

Tutti i pc delle varie postazioni, richiedono, all'accensione, la password, prima di avviare i programmi. L'attivazione della "condivisione" dei dati contenuti nei pc delle varie postazioni di lavoro collegate in rete è limitata solo alle cartelle che non contengono dati personali.

La consegna delle password ai responsabili del trattamento dei dati viene effettuata in forma riservata, dall'Amministratore di Sistema con raccomandazione alla custodia.

Viene, altresì disposto il cambiamento delle password ad ogni trimestre.

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

Elenco dei trattamenti di dati personali (regola 19.1 disciplinare tecnico)

Finalità del trattamento

Il trattamento dei dati personali è funzionale al raggiungimento delle finalità di istruzione e di formazione in ambito scolastico, professionale e superiore, con particolare riferimento a quelle svolte anche in forma integrata, ed è quindi di **rilevante interesse pubblico, ai sensi degli articoli 20, 21, 95, 96 del D.lgs 196/2003.**
Per le sue finalità istituzionali, l'Istituzione scolastica tratta dati personali, sia comuni, sia sensibili o giudiziari, di studenti, genitori, personale dipendente e fornitori.

BANCHE DATI TRATTATI DAI DOCENTI

I dati personali trattati dai docenti sono contenuti in banche dati su supporto cartaceo e/o informatico che si classificano in:

- basi di dati alle quali hanno accesso più docenti
- basi di dati alle quali ha accesso un solo docente

Le banche dati cui hanno accesso più docenti sono:

- il registro di classe
- il registro dei verbali del consiglio di classe o di interclasse
- la documentazione relativa alla programmazione didattica
- i documenti di valutazione
- i certificati medici degli allievi
- la corrispondenza con le famiglie
- la documentazione dello stato di handicap

Le banche dati cui ha accesso il singolo docente sono:

- il registro personale

- gli elaborati

BANCHE DATI TRATTATI DAL PERSONALE ATA

Le banche dati su supporto cartaceo e/o informatizzato, contenenti dati personali, cui ha accesso il personale di segreteria, raggruppati in insiemi omogenei, sono:

- i fascicoli relativi al personale della scuola
- i fascicoli degli alunni e ex alunni
- l'anagrafe fornitori, i contratti
- la documentazione finanziaria e contabile
- i verbali delle Assemblee degli Organi Collegiali
- i fascicoli del Personale Direttivo, Docente e Amministrativo
- la documentazione didattica trattata dai docenti per la conservazione
- i fascicoli del personale in prova

BANCHE DATI TRATTATI DAL DIRIGENTE SCOLASTICO

Le banche dati di pertinenza del Dirigente scolastico sono:

- la programmazione e gli atti relativi allo stato di disagio
- il protocollo riservato
- il registro degli infortuni

Nell'ambito delle banche dati sopra elencate, possono essere trattati dati sia **dati personali e identificativi**, sia **dati sensibili e giudiziari**, ai sensi del regolamento UE 679/2016

Elenco dei trattamenti di dati personali

La tipologia dei dati sensibili e giudiziari che possono essere trattati dalle scuole, nonché gli ambiti in cui tali dati possono emergere e i soggetti ai quali possono essere comunicati, sono stati **tassativamente previsti dal Regolamento del MPI (D.M. 305/2006).**

Nella **tabella** che segue, con riferimento al sopra richiamato Regolamento, si riportano:

- gli ambiti del trattamento e/o i processi in cui possono emergere dati sensibili e giudiziari, con riferimento al Regolamento MPI (con indicazione del numero della scheda allegata al Regolamento);
- i tipi di dati trattati;
- i terzi a cui è possibile comunicare i dati sensibili e giudiziari.

Per completezza, si allegano le schede del Regolamento MPI, che fanno parte integrante del presente documento. **Tab. 1 - Elenco dei trattamenti (regola 19.1 del disciplinare tecnico)**[1]

Legenda:
Schede = **sono** le schede allegate al Regolamento MPI n. 305/2006, allegate anche al presente DPS
C = dati comuni - **S** = dati sensibili - **G** = dati giudiziari

[1] Fonte: Modello Garante Privacy con adattamento.

Descrizione sintetica del trattamento			Natura dei dati			ID Struttura di riferimento *(v. Tab. 2)*	ID Altre strutture coinvolte *(v. Tab. 2)*	Terzi a cui vengono comunicati i dati e indicazioni delle finalità del trattamento di dati sensibili e giudiziari (*vedi schede allegate al Regolamento MPI*)
Id Trattamento	**Ambito del trattamento e/o processo gestito**	**Interessati**	**S**	**G**	**C**			
T1	**Gestione Area Alunni** Relativamente ai dati sensibili e giudiziari : • **Scheda n. 4** – Attività propedeutiche all'avvio dell'anno scolastico; • **Scheda n. 5** – Attività educativa, didattica e formativa e di valutazione; • **Scheda n. 7** – Rapporti Scuola-Famiglie: gestione del contenzioso.	**Alunni Genitori**	**x**	**x**	**x**	**A2.2**	**A5 – A3.1 –A7**	- agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgsl. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio; - ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio; - alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente la carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio; - agli Istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile; - all'INAIL per la denuncia di infortuni ex-D.P.R. 30 giugno 1965, n. 1124; - alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro di istituto per l'Handicap e per la predisposizione e la verifica del Piano Educativo Individuale, ai sensi della Legge 5 febbraio 1992, n.104; - ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro, ai sensi della Legge 24 giugno 1997, n. 196 e del D. Lgsl. 21 aprile 2005, n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio. - Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia; - Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia; - Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza.
T2	**Gestione Area Bilancio**	**Personale Fornitori**			**x**	**A3.2**		USP, USR, MPI, Agenzia delle Entrate, Altre istituzioni scolastiche, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Banca che effettua il servizio di cassa

Descrizione sintetica del trattamento			Natura dei dati			ID Struttura di riferimento *(v. Tab. 2)*	ID Altre strutture coinvolte *(v. Tab. 2)*	Terzi a cui vengono comunicati i dati e indicazioni delle finalità del trattamento di dati sensibili e giudiziari (*vedi schede allegate al Regolamento MPI*)
Id Trattamento	**Ambito del trattamento e/o processo gestito**	**Interessati**	**S**	**G**	**C**			
T3	**Gestione Area Personale** Relativamente ai dati sensibili e giudiziari : • **Scheda n. 1** – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro; • **Scheda n. 2** – Gestione del contenzioso e procedimenti disciplinari; • **Scheda n. 3** – Organismi collegiali e commissioni istituzionali; • **Scheda n. 7** – Rapporti Scuola-Famiglie: gestione del contenzioso.	**Personale**	**x**	**x**	**x**	**A1.1 – A3.1**	**A1.2 – A2.3 – A3.2 - A1.3**	- Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego; - Organi preposti al riconoscimento della causa di servizio/equo indennizzo, ai sensi del DPR 461/2001); - Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (d.lg. n. 626/1994) - Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del d.P.R. n. 1124/1965; - Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della L. 68/1999; - Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali; - Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità; - Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge 18 luglio 2003, n. 186; - Organi di controllo (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex Legge n. 20/94 e D.P.R. 20 febbraio 1998, n.38; - Agenzia delle Entrate: ai fini degli obblighi fiscali del personale ex Legge 30 dicembre 1991, n. 413; - MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335; - Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art. 50, comma 3, d.lg. n. 165/2001). - Ministero del Lavoro e delle Politiche Sociali: per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi a Collegi di conciliazione ex D.Lgs. 30 marzo 2001, n. 165; - Organi arbitrali: per lo svolgimento delle procedure arbitrali ai sensi dei CCNL di settore; - Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di giustizia; - Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria: per l'esercizio dell'azione di giustizia; Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale. - USP, USR, MPI, Altre istituzioni scolastiche, Organi preposti agli accertamenti idoneità impiego

Descrizione sintetica del trattamento			Natura dei dati			ID Struttura di riferimento *(v. Tab. 2)*	ID Altre strutture coinvolte *(v. Tab. 2)*	Terzi a cui vengono comunicati i dati e indicazioni delle finalità del trattamento di dati sensibili e giudiziari (*vedi schede allegate al Regolamento MPI*)
Id Trattamento	**Ambito del trattamento e/o processo gestito**	**Interessati**	**S**	**G**	**C**			
T4	**Gestione Area Retribuzioni** Relativamente ai dati sensibili e giudiziari : • **Scheda n. 1** – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro; • **Scheda n.** 2 – Gestione del contenzioso e procedimenti disciplinari; • **Scheda n. 3** – Organismi collegiali e commissioni istituzionali;	**Personale**	**x**	**x**	**x**	**A1.2**	**A3.2**	- Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego; - Organi preposti al riconoscimento della causa di servizio/equo indennizzo, ai sensi del DPR 461/2001); - Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (d.lg. n. 626/1994) - Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del d.P.R. n. 1124/1965; - Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della L. 68/1999; - Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali; - Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità; - Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge 18 luglio 2003, n. 186; - Organi di controllo (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex Legge n. 20/94 e D.P.R. 20 febbraio 1998, n.38; - Agenzia delle Entrate: ai fini degli obblighi fiscali del personale ex Legge 30 dicembre 1991, n. 413; - MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335; - Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art. 50, comma 3, d.lg. n. 165/2001). - Ministero del Lavoro e delle Politiche Sociali: per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi a Collegi di conciliazione ex D.Lgs. 30 marzo 2001, n. 165; - Organi arbitrali: per lo svolgimento delle procedure arbitrali ai sensi dei CCNL di settore; - Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di giustizia; - Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria: per l'esercizio dell'azione di giustizia; Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale. - USP, USR, MPI, Altre istituzioni scolastiche, Organi preposti agli accertamenti idoneità impiego Banca che effettua il servizio di cassa

Descrizione sintetica del trattamento			Natura dei dati			ID Struttura di riferimento *(v. Tab. 2)*	ID Altre strutture coinvolte *(v. Tab. 2)*	Terzi a cui vengono comunicati i dati e indicazioni delle finalità del trattamento di dati sensibili e giudiziari (*vedi schede allegate al Regolamento MPI*)
Id Trattamento	**Ambito del trattamento e/o processo gestito**	**Interessati**	**S**	**G**	**C**			
T5	**Gestione Fiscale**	**Personale**			**x**	**A1.2**	**A3.2**	**USP, MPI, Agenzia delle Entrate, Corte dei Conti, Enti assistenziali, previdenziali e assicurativi, MEF, Banca che effettua il servizio di cassa**
T6	**Gestione Protocollo** Relativamente ai dati sensibili e giudiziari: Tutte le schede allegate al regolamento sul trattamento dei dati sensibili e giudiziari	**Alunni, Genitori, Fornitori, Personale, Altre amministrazioni**	**X**	**x**	**x**	**A1.3**		USP, USR, MPI, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Agenzia delle Entrate, Organi preposti agli accertamenti idoneità impiego, Banca che effettua il servizio di cassa
T7	**Gestione Sicurezza**	**Personale amministrativo accesso aree Axios**			**x**	**A4**	**A3.2**	MPI
T8	**Backup e Restore**	**Banca dati Amministrativa**			**x**	**A4**	**A3.2**	

Descrizione sintetica del trattamento			Natura dei dati			ID Struttura di riferimento *(v. Tab. 2)*	ID Altre strutture coinvolte *(v. Tab. 2)*	Terzi a cui vengono comunicati i dati e indicazioni delle finalità del trattamento di dati sensibili e giudiziari (*vedi schede allegate al Regolamento MPI*)
Id Trattamento	**Ambito del trattamento e/o processo gestito**	**Interessati**	**S**	**G**	**C**			
T9	**Gestione Protocollo e corrispondenza riservata** Relativamente ai dati sensibili e giudiziari: **Tutte le schede** allegate al regolamento sul trattamento dei dati sensibili e giudiziari	**Alunni, genitori, personale**	**x**	**x**	**x**	**A3.1**		USP, MPI, Altre istituzioni scolastiche, AUSL, Enti Locali, Gestori pubblici e privati dei servizi di assistenza, Istituti di assicurazione, INAIL, Aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola lavoro, Avvocature dello Stato, Magistrature ordinarie e amministrativo-contabile, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Organi di polizia giudiziaria, Liberi professionisti
T10	**Gestione della posta elettronica**	**Personale, utenti del servizio scolastico, fornitori**			**x**	**A1.1**	**A1.3**	
T11	**Gestione Scioperi del Personale dipendente** Relativamente ai dati sensibili e giudiziari : **Scheda A** – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro;	**Personale**	**x**		**x**	**A1.1**	**A1.3**	**https://websptnet.tesoro.it/SCIOPNET**

Descrizione sintetica del trattamento			Natura dei dati			ID Struttura di riferimento *(v. Tab. 2)*	ID Altre strutture coinvolte *(v. Tab. 2)*	Terzi a cui vengono comunicati i dati e indicazioni delle finalità del trattamento di dati sensibili e giudiziari (*vedi schede allegate al Regolamento MPI*)
Id Trattamento	**Ambito del trattamento e/o processo gestito**	**Interessati**	**S**	**G**	**C**			
T12	**Gestione Anagrafe delle prestazioni**	**Personale interno ed esterno, Fornitori**			**x**			**www.anagrafeprestazioni.it**
T13	**Invio documenti tramite Entratel e DM10**	**Personale esterno e della scuola**			**x**	**A1.2**	**A3.2**	**Sito entratel**
T14	**Gestione Pre 96**	**Personale**			**x**	**A1.2**	**A3.2**	**Ragioneria Provinciale del Tesoro**
T15	**Gestione INPS**	**Personale**	**X**		**x**	**A1.2**	**A3.2**	**INPS**
T16	**Gestione con Suite Microsoft Office comunicazione**	**Personale interno ed esterno, Fornitori**			**x**	**Tutte**	**Tutte**	
T17	**Gestione Dispostivi dell'infrastruttura tecnologica**	**Personale interno ed esterno, Fornitori**			**x**	**A4**		

Descrizione sintetica del trattamento			Natura dei dati			ID Struttura di riferimento *(v. Tab. 2)*	ID Altre strutture coinvolte *(v. Tab. 2)*	Terzi a cui vengono comunicati i dati e indicazioni delle finalità del trattamento di dati sensibili e giudiziari (*vedi schede allegate al Regolamento MPI*)
Id Trattamento	**Ambito del trattamento e/o processo gestito**	**Interessati**	**S**	**G**	**C**			
T18	**Gestione Provvedimenti Disciplinari alunni** Relativamente ai dati sensibili e giudiziari : **Scheda B** – Attività propedeutiche all'avvio dell'anno scolastico; **Scheda n. E** – Attività educativa, didattica e formativa e di valutazione; **Scheda n. F** – Rapporti Scuola-Famiglie: gestione del contenzioso.	**Genitori, Alunni, Personale**	**x**	**x**	**x**	**A3.3**	**A1.3**	**Genitori, USP** a) agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgsl. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio; b) ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio; **c)** alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la predisposizione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104;
T21	**Contratti prestazione**	**Personale ed esterno**			**x**	**A1.4**	**A1.3 – A1.2**	**INAIL, Ditte Esterne**
T23	**Gestione Archivio cartaceo storico**	**Tutte le categorie**	**x**	**x**	**x**	**A5**		

Descrizione sintetica del trattamento			Natura dei dati			ID Struttura di riferimento *(v. Tab. 2)*	ID Altre strutture coinvolte *(v. Tab. 2)*	Terzi a cui vengono comunicati i dati e indicazioni delle finalità del trattamento di dati sensibili e giudiziari (*vedi schede allegate al Regolamento MPI*)
Id Trattamento	**Ambito del trattamento e/o processo gestito**	**Interessati**	**S**	**G**	**C**			
T24	**Gestione Assistenza e manutenzione hardware**	**Soggetti interni e terzi che utilizzano i PC degli uffici Amministrativi**	**X**	**x**	**x**	**A4**		
T25	**Gestione titolario Generale**				**x**	**A1.3**		**USP, USR, MPI**
T26	**Gestione Riproduzione e notifica documenti**	**Personale, Alunni, Genitori Fornitori**	**X**	**x**	**x**	**A7**		
T28	**Gestione Inventario e Fornitori di beni e servizi**	**Ditte esterne**			**x**	**A2.1**	**A3.1**	**Ditte esterne**

Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati (regola 19.2 disciplinare tecnico)

Il **titolare del trattamento** ha designato, con atto scritto contenente analitiche istruzioni relative ai compiti affidati:

- il **responsabile del trattamento dei dati, nella persona dell'ins. Gerlando Alonge, Docente interno (Esperto della privacy)**

Il responsabile del trattamento provvede, sulla base della lettera di designazione, ad individuare gli **incaricati del trattamento** dei dati personali appartenenti ai profili professionali del personale ATA; ha conferito agli stessi l'incarico con atto scritto contenente puntuali istruzioni relative agli ambiti di trattamento consentiti, corredato da linee guida e con allegate le schede relative al trattamento dei dati sensibili e giudiziari.

Il titolare provvede ad individuare e **incaricare il personale docente** con atto che fornisce le istruzioni necessarie.

I singoli incaricati, che hanno rilasciato ricevuta della avvenuta consegna della lettera di incarico, sono stati informati che l'ambito dei trattamenti autorizzati è suscettibile di aggiornamento periodico e che devono:

- trattare i dati comuni (non sensibili e giudiziari) per i soli fini istituzionali della scuola;
- comunicare i dati comuni a terzi nei soli casi previsti da leggi o regolamenti;
- trattare i dati sensibili e giudiziari nei soli casi previsti da norme di legge o dal Regolamento MPI sul trattamento dei dati sensibili e giudiziari;
- comunicare i dati sensibili e giudiziari a terzi, se di competenza, nei soli casi previsti da norme di legge o dal Regolamento MPI sul trattamento dei dati sensibili e giudiziari;
- diffondere i dati sensibili e giudiziari a terzi, se di competenza, nei soli casi previsti da norme di legge o dal Regolamento MPI sul trattamento dei dati sensibili e giudiziari.

Agli incaricati è stato consegnata copia del Regolamento MPI sul trattamento dei dati sensibili e giudiziari, adottato dall'Istituzione scolastica.

La comunicazione dei soggetti responsabili e incaricati è avvenuta attraverso la pubblicazione all'albo della scuola dell'organigramma della scuola e delle responsabilità.

A tutti gli incaricati del trattamento di dati mediante strumento elettronico sono state conferite credenziali di autenticazioni (art.34, comma 1, lett.b Codice privacy) mediante parola chiave, conformi alle caratteristiche indicate nell'allegato B Codice privacy. Agli incaricati sono state fornite puntuali indicazioni per la modifica della parola chiave.

Si riporta di seguito la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati **(Tabella 2).**

Tab. 2 - Distribuzione dei compiti e delle responsabilità – soggetti preposte ai trattamenti (regola 19.2, discip. tecnico)[2]

Id Struttura	*Struttura o soggetti incaricati (esempi)*	*Trattamenti effettuati (v. Tab. 1)*	*Descrizione dei compiti e delle responsabilità*
A1.1	**Ufficio Personale**	**T3 – T10 – T11**	• **Uso applicativo Area amministrativa** • **Gestione dei documenti office** • **Accesso all'area riservata del sito Istruzione** • **Gervizio di gestione degli scioperi** • **Gestione, archiviazione, consultazione dei fascicoli personali dei dipendenti** • **Gestione del software per la rilevazione delle presenze del personale** • **Gestione della posta elettronica**
A1.2	**Ufficio Contabilità**	**T2 – T13 –T14**	• **Uso applicativo Area contabilità** • **Gestione dei documenti office** • **Accesso all'area riservata del sito Istruzione** • **Gestione della documentazione cartacea relativa al bilancio** • **Invio Documenti Entratel** • **Invio DMA**
A1.3	**Ufficio Protocollo**	**T6**	• **Uso applicativo Area protocollo** • **Gestione dei documenti office** • **Stampe registro protocollo** • **Smistamento e archiviazione corrispondenza**
A2.1	**Ufficio affari generali**	**T28**	• **Gestione dei documenti office** • **Tenuta Inventario beni** • **Rapporti con i fornitori** • **Gare e acquisti di beni e servizi**
A2.2	**Ufficio Didattica Alunni**	**T1**	• **Utilizzo dell'applicativo Area Alunni** • **Gestione dei documenti di office automation** • **Accesso all'area del sito** www.istruzione.it • **Accesso al servizio di denuncia infortuni** • **Consultazione e archiviazione dei fascicoli personali degli alunni**

[2] Fonte: Modello Garante Privacy con adattamento.

Id Struttura	*Struttura o soggetti incaricati (esempi)*	*Trattamenti effettuati (v. Tab. 1)*	*Descrizione dei compiti e delle responsabilità*
A3.1	**Ufficio Dirigente Scolastico**	**T22 -T9**	• **Gestione degli Organi collegiali** • **Gestione dell'offerta formativa** • **Gestione della sicurezza sul posto di lavoro D.lgs. 81/2008** • **Gestione della protezione dei dati personali** • **Relazioni sindacali** • **Rapporti con gli enti** • **Gestione Protocollo Riservato**
A3.2	**Ufficio Direttore Servizi Generali e Amministrativi**	**T1-T2-T3-T4-T5-T6-T7**	• **Gestione del Bilancio** • **Coordinamento operazioni relative alle disposizioni sulla privacy** • **Gestione rapporti con il personale** • **Organizzazione del Lavoro ATA** • **Concessione credenziali accesso area riservata Istruzione.it**
A3.3	**Collaboratore del D.S.**	**T18**	• **Gestione Provvedimenti disciplinari alunni** • **Rilevazione assenze alunni della scuola**
A4	**Amministratore di Sistema**	**T8 - T17 –T24**	• **Amministrazione del Server di sistema** • **Amministrazione sistemi operativi dei clients in rete** • **Amministrazione e configurazione router per l'accesso ad internet** • **Gestione automazione del backup** • **Installazione su client e su HW della rete amministrativa di SW di sicurezza antispywere e antivirus** • **Aggiornamento software e password**
A5	**Personale Docente**	**T1**	• **Trattamento dati degli alunni a loro affidati**
A6	**Archivio**	**T23 – T27**	• **Gestione e archiviazione Atti Amministrativi dell'Istituzione Scolastica**
A7	**Collaboratori scolastici**	**T26**	• **Fotocopiatura di documenti** • **Prelevamento e distribuzione fax** • **Notifica di documenti** • **Trasporto di documenti**

ELENCO DELLE BANCHE DATI E TRATTAMENTI

a. Banca dati Alunni *(computer – Ufficio alunni)*

dati sensibili: P.E.I., Profilo Diagnostico Funzionale, scelta religione, dati nascita, documenti sanitari, riconoscimento di esonero, agevolazioni, sanzioni, schede di valutazione;

supporto informatico: inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, certificati vari, gestione SISSI e INTRANET, statistiche, trasmissione e-mail, Relazioni osservative, P.E.I., Profilo Diagnostico Funzionale.

sistema di backup e frequenza: supporto CD tramite masterizzatore, frequenza settimanale.

b. Banca dati Genitori*(computer ufficio alunni):*

dati sensibili: documenti sanitari, domande di buono libri, domande di borse di studio, domande di contributi, separazioni, trattamenti cautelari**;**

supporto informatico: inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, elaborazione elenchi per elezioni interne OO.CC, gestione SISSI e INTRANET, statistiche, trasmissione e-mail

sistemi hardware che trattano l'archivio: server ARGO, computer rete amministrativa compresi i computer laptop;

sistema di backup e frequenza: supporto CD tramite masterizzatore, frequenza settimanale;

c. Banca dati Personale Direttivo *(computer DSGA)****:***

dati sensibili: adesione a sindacati, documenti sanitari;

supporto informatico: inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, rilascio certificati vari, gestione ARGO e INTRANET, statistiche, trasmissione e-mail

sistema di backup e frequenza: supporto CD tramite masterizzatore, frequenza settimanale;

d. Banca dati Personale Docente *(computer Ufficio personale):*

dati sensibili: adesione a sindacati, documenti sanitari, riconoscimento di esonero, agevolazioni, sanzioni;

supporto informatico: inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, rilascio certificati vari, gestione ARGO e INTRANET, statistiche, trasmissione e-mail

sistema di backup e frequenza: supporto CD tramite masterizzatore, frequenza settimanale;

e. Banca dati Personale ATA *(computer Ufficio personale):*

dati sensibili: adesione a sindacati, documenti sanitari, riconoscimento di esonero, agevolazioni, sanzioni;

supporto informatico: inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, rilascio certificati vari, gestione ARGO e INTRANET, statistiche, trasmissione e-mail;

sistema di backup e frequenza: supporto CD tramite masterizzatore, frequenza settimanale;

f. Banca dati Soggetti che sviluppano e prestano opera di collaborazione con la scuola *(computer DSGA):*

dati sensibili: adesione a sindacati, documenti sanitari;

supporto informatico: inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, rilascio certificati vari, gestione ARGO e INTRANET, statistiche, trasmissione e-mail;

sistema di backup e frequenza: supporto CD tramite masterizzatore, frequenza settimanale;

g. Banca dati Fornitori *(computer DSGA):*

dati sensibili: adesione a sindacati, documenti sanitari;

supporto informatico: inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, rilascio certificati vari, gestione ARGO e INTRANET, statistiche, trasmissione e-mail;

sistema di backup e frequenza: supporto CD tramite masterizzatore, frequenza settimanale;

RISORSE

Le risorse da proteggere si possono suddividere in 4 categorie:

- Luoghi Fisici (locali dove sono ubicate le risorse hardware che trattano o ospitano banche dati, gli archivi)
- Risorse hardware (server di rete, sistemi informatici su cui operano gli incaricati, modem, router, dispositivi di backup)
- Risorse software.

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

L'elenco degli eventi potenzialmente, individuato dal Garante, che comportano rischi per la sicurezza dei dati personali, è il seguente:

1) comportamenti degli operatori:

- sottrazione di credenziali di autenticazione*;*
- carenza di consapevolezza, disattenzione o incuria, errore materiale;
- comportamenti sleali o fraudolenti;

2) eventi relativi agli strumenti:

- azione di virus informatici o di programmi suscettibili di recare danno, spamming o tecniche di sabotaggio, malfunzionamento, indisponibilità o degrado degli strumenti, accessi esterni non autorizzati, intercettazione di informazioni in rete;

3) eventi relativi al contesto fisico-ambientale:

- ingressi non autorizzati a locali/aree ad accesso ristretto, sottrazione di strumenti contenenti dati, eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ...), nonché dolosi, accidentali o dovuti ad incuria, guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.), errori umani nella gestione della sicurezza fisica*.*

La ricognizione e l'analisi dei rischi, che potrebbero comportare una distruzione, sottrazione, perdita, trattamento abusivo dei dati, di origine dolosa, colposa, ovvero meramente fortuita, in grado di recare pregiudizio ai dati personali trattati, è stata riportata nelle tabelle che seguono.

Tab. 3 – Analisi dei rischi (regola 19.3 del disciplinare tecnico)[3]

	Id Rischio	*Rischi*	*Si/No*	*Descrizione dell'impatto sulla sicurezza (gravità:alta/media/bassa)*
Comportamento degli operatori	**R1**	**Sottrazione di credenziali di autenticazione.**	**Si**	**Alta**
	R2	**Carenza di consapevolezza, disattenzione o incuria.**	**Si**	**Media**
	R3	**Comportamenti sleali o fraudolenti.**	**Si**	**Bassa**
	R4	**Errore materiale.**	**Si**	**Media**
Eventi relativi agli strumenti	**R5**	**Azione di *virus* informatici o di programmi suscettibili di recare danno.**	**Si**	**Alta**
	R6	***Spamming* o tecniche di sabotaggio.**	**Si**	**Alta**
	R7	**Malfunzionamento, indisponibilità o degrado degli strumenti.**	**Si**	**Media**
	R8	**Accessi esterni non autorizzati.**	**Si**	**Media**
	R9	**Intercettazione di informazioni in rete.**	**Si**	**Media**
Eventi relativi al contesto	**R10**	**Accessi non autorizzati a locali/reparti ad accesso ristretto.**	**Si**	**Bassa**
	R11	**Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc,) nonché dolosi, accidentali o dovuti ad incuria.**	**Si**	**Media**
	R12	**Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.).**	**Si**	**Media**
	R13	**Errori umani nella gestione della sicurezza fisica.**	**Si**	**Media**

[3] Fonte: Modello Garante Privacy con adattamento.

Misure in essere e\o da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità (*regola 19.4*)

Misure generali (istruzioni impartite agli incaricati)

Misure per l'integrità e la disponibilità dei dati	• I singoli incaricati devono assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso loro esclusivo. • Oltre alla custodia personale delle credenziali assegnate, copia di esse deve essere depositata al protocollo riservato del Dirigente Scolastico e nella cassaforte in gestione del D.S.G.A. • Al termine della giornata lavorativa del venerdì, i singoli incaricati. provvederanno a effettuare il salvataggio dei dati su supporti movibili che verranno custoditi dal D.S.G.A.
Protezione delle aree e dei locali finalizzati alla custodia e accessibilità dei dati	• Il trattamento di dati personali con strumenti elettronici è consentito mediante credenziali di autenticazione (cioè mediante un codice per l'identificazione associato a una parola chiave riservata per ogni singolo incaricato e conosciuta solamente dai singoli incaricati) • I singoli incaricati devono adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso loro esclusivo. In particolare, oltre alla custodia personale delle credenziali assegnate, copia di esse deve essere depositata al protocollo riservato del Dirigente Scolastico e nella cassaforte in gestione • Ogni 6 mesi i singoli incaricati modificheranno codice e parola chiave delle credenziali garantendo i livelli di segretezza dovuti • In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi • Durante la sessione di trattamento, lo strumento elettronico non deve essere accessibile ad altri soggetti estranei all'incarico assegnato • I singoli incaricati sono tenuti al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali situati negli 'apposito e riservati arredi d'ufficio. A tal fine l'accesso agli archivi non deve essere consentito ad altri soggetti estranei all'incarico assegnato. • Durante il trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dai singoli incaricati fino alla ricollocazione in archivio in maniera che ad essi non accedano persone prive di autorizzazione. • L'accesso agli archivi contenenti dati sensibili deve essere controllato. Non è ammesso l'accesso all'archivio a persone, a qualunque titolo, dopo l'orario di chiusura dell'ufficio

MISURE MINIME DI SICUREZZA

In questa parte del documento vengono descritte le misure adottate per contrastare i rischi individuati a seguito dell'analisi effettuata e della valutazione degli eventi. Per misura si intende, non solo lo specifico intervento tecnico o organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi a una specifica minaccia, ma anche tutte quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

Protezione di aree e locali

Durante l'orario di apertura è in funzione un servizio di portineria, per l'ingresso principale. L'accesso ai locali dove avviene il trattamento è consentito al solo personale autorizzato tramite porte dotate di serratura. L'edificio scolastico è provvisto di luci d'emergenza e dispositivi antincendio : idranti, estintori in polvere ABC da Kg 6.00, estintori a $C0_2$ in prossimità dei quadri elettrici. Tutti gli elaboratori hanno un sistema di continuità dell'alimentazione elettrica.

Archiviazione e custodia di atti, documenti e supporti

Tutti gli uffici sono attrezzati con armadi dotati di serrature e accessibili al solo personale autorizzato, per l'archiviazione e custodia della documentazione cartacea, organizzata in fascicoli. Gli uffici del D.S. e del D.S.G.A. sono dotati di cassaforte per la custodia di atti e documenti di particolare rilevanza.

Misure logiche di sicurezza

Ogni utente è informato delle norme e delle procedure che regolano l'utilizzo degli strumenti informatici.

Il personale tecnico preposto alle manutenzioni proveniente dall'esterno può operare solo alla presenza del personale interno dei servizi informatici. I server sono dotati di un sistema centrale di rilevazione dei virus informatici, di accesso a internet e di condivisione di file all'interno della rete dell'Istituto. L'aggiornamento avviene in un periodo non superiore ai 15 giorni.

Su ogni elaboratore è installato un sistema di rilevazione di virus informatici che è aggiornato con una periodicità non superiore ai 7 giorni.

A ogni utente sono assegnati un codice identificativo e una password personali; la password ha una validità di 3 mesi.

Il codice identificativo e la password abilitano all'accesso delle risorse di rete e all'uso delle aree di lavoro sulla base delle autorizzazioni assegnate al singolo utente o al gruppo di lavoro (profilo comune) a cui partecipa.

L'amministratore di sistema, dietro indicazione e mandato della dirigenza, gestisce e vigila su codici identificativi e password assegnate agli utenti, provvede alla disattivazione dei codici e delle password di utenti cessati, disattiva i codici e le password smarrite o erroneamente distribuite, ovvero divulgate ad altri utenti.

Le varie funzioni dell'Istituto utilizzano differenti software gestionali che operano sulle basi di dati trattate dall'Istituto. Ogni software gestionale consente il trattamento dei soli dati necessari e sufficienti allo svolgimento delle attività dell'operatore.

Il personale docente, con accesso codificato e protetto da password sul web, ha il permesso di assegnare le valutazioni agli studenti, sia in corso d'anno (voti per prove scritte e orali) sia nei periodi di valutazione intermedia e finale.

I fornitori non hanno accesso alle postazioni ed ai dati.

È il responsabile della gestione e della sicurezza del sistema informatico, su indicazione della dirigenza, che abilita gli utenti ad accedere a internet, vigila sul traffico in

ingresso e uscita e sugli accessi procedendo all'eventuale disattivazione.

L'accesso è protetto da sistemi anti-intrusione a più livelli.

Il responsabile della gestione e della sicurezza del sistema informatico è l'Amministratore di Sistema, nella persona della Sig. ra Faseli Vincenza.

Per tutti gli elaboratori sono previste attività periodiche di manutenzione per l'aggiornamento dei sistemi da parte dei produttori di software e hardware.

Misure periodiche

Il Dirigente Scolastico, in qualità di rappresentante legale dell'Istituzione scolastica (Titolare al trattamento dei dati ai sensi dell'art. 4, lettera f, del Codice) e il Responsabile del trattamento verificano il rispetto delle istruzioni impartite agli incaricati e delle misure di sicurezza adottate dalla scuola. Più in generale, si vigilerà affinché il trattamento effettuato dalla scuola sia sempre compreso nelle sue finalità istituzionali e, per nessuna ragione, prescinda da queste.

Vengono indicate, sinteticamente, le principali misure adottate nella seguente tabella:

MISURA	RISCHI CONTRASTATI	TRATTAMENTI INTERESSATI	STRUTTURA
Istruzioni agli incaricati	Accessi non autorizzati	Tutti	Responsabili del trattamento
Incarichi di responsabilità	Deresponsabil.ne	Tutti	Idem
Formazione	Accessi; visione Virus;	Dati di alunni e personale	Personale
Installazione antivirus	Danneggiamento dati informatici	Tutti	DSGA, Amministrati-vi
Potenziamento sicurezza edifici(1)	Incendi ed infiltrazioni	Tutti	Dir. Scolastico DSGA Pers. ATA
Istituzione di Password	Accesso ai dati Informatici	Tutti	Responsabili, DSGA, Amministrativi
Installazione gruppi di continuità(2)	Danneggiamento banche dati informatici	Tutti	Responsabili del trattamento
Circolari	Diffusione di dati	Alunni e famiglie	Docenti e coll. Scolastici

(1) trattasi di richieste di intervento da avanzare all'ente locale competente:
(2) eventualmente da richiedere all'ente locale competente.

Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento (regola 19.5)

Backup	• Al termine della giornata lavorativa del venerdì, i singoli incaricati [*o l'Amministratore di sistema]* provvederanno a effettuare il backup dei dati su supporti movibili, tramite procedura pianificata di backup attivata sui PC *[evidenziare se presente anche una procedura di backup automatica su server],* che verranno custoditi dal Responsabile *[ovvero dall'incaricato se previsto dalla lettera di incarico]*
Ripristino	• Il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento avverrà mediante l'utilizzo degli appositi backup

Criteri e procedure per il salvataggio dei dati (regola 19.5 del disciplinare tecnico)

Salvataggio\Backup			
Banca dati	***Criteri e procedure per il Backup***	***Luogo di custodia delle copie***	***Struttura o soggetti incaricati del salvataggio***
SISSI\Server	Tramite applicativo automatizzato su server	Cassaforte conforme alle regole di sicurezza	I singoli incaricati [*o l'Amministratore di Sistema*]
Documenti di Office automation *[Windows Office o altri]* su hard-disk dei PC	Copia archivi PC su supporto C-RW/DVD, tramite attività panificata	Cassaforte conforme alle regole di sicurezza	I singoli incaricati [*o l'Amministratore di Sistema*]
Documenti Posta elettronica su su hard-disk dei PC	Copia archivi PC su supporto C-RW/DVD, tramite attività panificata	Cassaforte conforme alle regole di sicurezza	I singoli incaricati [*o l'Amministratore di Sistema*]

Criteri e procedure per il ripristino della disponibilità dei dati (regola 19.5 del disciplinare tecnico)

Ripristino		
Banca dati / archivio dati	***Criteri e procedure per il salvataggio e il ripristino dei dati***	***Pianificazione delle prove di ripristino***
SISSI	In caso di assenza\impossibilità dell'incaricato o dell'amm. di sistema, il DSGA o il DS autorizzano un altro incaricato per il ripristino entro sette giorni dalla perdita dei dati)	Quindicinale/mensile/..
Documenti di Office automation *[Windows Office o altri]* su hard-disk dei PC	Tramite procedure di restore da supporto C-RW/DVD (in caso di assenza\impossibilità dell'incaricato o dell'amm. di sistema, il DSGA o il DS autorizzano un altro incaricato per il ripristino entro sette giorni dalla perdita dei dati)	Quindicinale/mensile/..
Documenti Posta elettronica su su hard-disk dei PC	Tramite procedure di restore da supporto C-RW/DVD (in caso di assenza\impossibilità dell'incaricato o dell'amm. di sistema, il DSGA o il DS autorizzano un altro incaricato per il ripristino entro sette giorni dalla perdita dei dati)	Quindicinale/mensile/..

Previsione di interventi formativi degli incaricati del trattamento (regola 19.6)

Ai sensi del Regolamento UE 679/2016 e della regola 19.6 dell'allegato B) del Codice della privacy (disciplinare tecnico), sono pianificati i seguenti **interventi formativi**:

1. **Entro settembre-ottobre di ogni anno**: eventuale aggiornamento del personale in caso di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali, per renderli edotti sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano, sulle misure minime adottate dal titolare (min.: 2 ore di aggiornamento);
2. **Entro settembre – ottobre di ogni anno**: formazione per nuovi assunti o in caso di cambiamento di mansioni, per renderli edotti sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano, sulle misure minime adottate dal titolare (min.: 4 ore di formazione].

Cifratura dei dati o separazione dei dati sensibili da quelli identificativi (regola 19.8)

Criteri da adottare per la cifratura o per la separazione dei dati sullo stato di salute dagli altri dati personali dell'interessato	Trasmissione dei dati personali limitatamente alle generalità "cognome e nome" ovvero ai soli dati essenziali richiesti specificamente trattati esclusivamente con lettere iniziali o con codici sanitari previsti da protocolli I dati personali trattati in database prevedono apposite schede che estrapolino solo le generalità escludendo, se non necessari, altri dati quali indirizzi, recapiti, scelte religiose. Le certificazioni mediche sullo stato di salute o sulle situazioni di handicap sono tenuti separati dagli altri dati, in busta chiusa sigillata, riportante sul fronte il solo riferimento a codici da cui non è possibile dedurre il contenuto.

Criteri per il salvataggio dei dati (copie di sicurezza)

Periodicamente verranno effettuate le copie di backup di tutti i dati posseduti dalla scuola e verrà anche stabilito un piano settimanale di verifica della correttezza ed immediata disponibilità delle copie di sicurezza effettuate. Ciascun assistente amministrativo è responsabile dell'effettuazione delle copie di backup del lavoro prodotto settimanalmente. Il coordinamento delle attività di salvataggio delle copie è affidato al DSGA**.**

Tutti i dati contenuti nei computer saranno settimanalmente memorizzati su CD-Rom riscrivibili che vengono etichettati, con indicazione della data di salvataggio. I CD-ROM vengono depositati nell'armadio blindato situato nella stanza del Direttore Amm.vo.

INTERVENTI DI COLLABORATORI ESTERNI, ESPERTI E SPECIALISTI

Nel caso in cui l'Istituzione scolastica si dovesse avvalere, per l'attuazione di interventi previsti dall'offerta formativa o dagli interventi miranti all'integrazione dei soggetti diversamente abili, della collaborazione di terapisti, esperti e specialisti, assistenti igienico-personali, è escluso, nei limiti del possibile, l'accesso dei medesimi a documentazioni contenenti dati sensibili. In merito alla possibilità di trattamento di dati personali particolari da parte dei suddetti soggetti, è previsto che i medesimi dichiarino:

1. di essere consapevoli degli obblighi previsti dal nuovo regolamento UE 679/2016 e dal D. L.vo 196/2003
2. di impegnarsi ad ottemperare all'obbligo di tutela dei dati personali
3. di adottare le istruzioni specifiche ricevute per la garanzia di sicurezza dei dati

APPENDICE

SCHEDE DEL REGOLAMENTO DATI SENSIBILI E GIUDIZIARI – MIUR Decreto Ministeriale n. 305 del 7 Dicembre 2006;

SCHEDA A

La *"scheda"* individua tutti i dati che possono essere oggetto di trattamento per le procedure di selezione, di reclutamento, di instaurazione, di gestione e di cessazione del rapporto di lavoro (*dati inerenti lo stato di salute, l'adesione a sindacati, quelli sulle convinzioni religiose per la concessione di permessi legati a particolari festività o per il reclutamento degli insegnanti di religione, i dati sulle convinzioni filosofiche o d'altro genere per eventuali connessioni con lo svolgimento del servizio di leva o come obiettore di coscienza, i dati di carattere giudiziario nell'ambito delle procedure concorsuali che coinvolgono l'interessato, le informazioni sulla vita sessuale connessi unicamente al caso eventuale della rettifica di attribuzione di sesso*); sono individuate, inoltre, le varie tipologie di trattamento possibili.

Indicazione del trattamento e descrizione riassuntiva del contesto

Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro:

— del personale dipendente dell'Amministrazione centrale e perifèrica del Ministero dell'istruzione, e dirigente, docente, educativo ed ATA delle istituzioni scolastiche ed educative, personale IRRE;
— dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato

Il trattamento concerne tutti i dati relativi alle procedure per la selezione e il reclutamento,all' instaurazione, alla gestione e alla cessazione del rapporto di lavoro.

1. I dati inerenti lo stato di salute sono trattati per: l'adozione di provvedimenti di stato giuridico ed economico, verifica dell'idoneità al servizio, assunzioni del personale appartenente alle c. d categorie protette, benefici previsti dalla normativa in tema di assunzioni, protezione della maternità, igiene e sicurezza sul luogo di lavoro, causa di servizio, equo indennizzo, onorificenze, svolgimento di pratiche assicurative, pensionistiche e previdenziali obbligatori e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce dì infortuni e/o sinistri e malattie professionali, fruizione di assenze, particolari esenzioni o permessi lavorativi per il personale e provvidenze, collegati a particolari condizioni di salute dell' interessato o dei suoi familiari, assistenza fiscale,mobilità territoriale, professionale e intercompartimentale;
2. I dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o *all'esercizio dei diritti sindacali;*

3. I dati sulle convinzioni religiose per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose. I dati sulle convinzioni religiose vengono in rilievo anche ai fini del reclutamento dei docenti di religione;
4. *I dati sulle convinzioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza;*
5. I dati di carattere giudiziario sono trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l' adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato.
6. le informazioni sulla vita sessuale possono desumersi unicamente in caso di eventuale rettificazione di attribuzione di sesso.

E' di seguito descritto sinteticamente il flusso informativo dei dati.

I dati sono raccolti su iniziativa degli interessati o previa richiesta dell'Ufficio presso i medesimi interessati, ovvero presso altri soggetti pubblici o privati, e sono trattati, sia in forma cartacea che telematica, per l'applicazione dei vari istituti disciplinati dalla legge e dai regolamenti in materia di selezione, reclutamento, gestione giuridica, economica, previdenziale, pensionistica, aggiornamento e formazione del personale.

Finalità di rilevante interesse pubblico perseguite

- **ART. 112:** *"instaurazione e gestione da parte **dei** soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale **o** temporaneo, e **di** altre forme di impiego che non comportano la **costituzione di un** rapporto di lavoro subordinato"*

- **ART. 62:** *"rilascio di documenti di riconoscimento";*

- **ART. 67:** *"attività di controllo e ispettive";*

- **ART 68:** " *applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;*

- **ART. 70:** *"applicazione della legge 8 luglio 1998 n. 230, e delle altre disposizioni di legge in materia obiezione di coscienza";*

- **ART. 72:** *rapporti con Enti di culto".*

- **ART.** ***73****: "supporto al collocamento e avviamento al lovoro.".*

Fonti normative

- ***Norme comuni:*** D.P.R. 10 gennaio 1957, n. 3; Legge 5 febbraio 1992, n. 104; Legge 12 marzo 1999, n. 68; D.Lgs. 30 marzo 2001, n. 165; Legge **15** luglio 2002, a. 145; R. D. 30 settembre 1922, n. 1290; Legge 24 maggio 1970, n. *336;* Legge 30 dicembre 1971, n. 1204; D.P.R. 29 dicembre 1973, n. 1032; D.P.R. 29 dicembre 1973, n. 1092; Legge 7 Febbraio 1979, n. 29; Legge *5* marzo 1990, n. 45; D.Lgs. 30 dicembre 1992, n. *503;* Legge 14 gennaio 1994, n. 20; Legge 8 agosto 1995, n. 335; D.P.R. 20 febbraio 1998, n. 38; Legge 12marzo 1999, n. 68; D.P.C.M. 20 dicembre 1999; Legge 8 marzo 2000, n. *53; D.*P.R. 29 ottobre 2001, n. 461.

- ***Norme relative al personale amministrativo del Ministero dell'Istruzione:*** legge n. 472/1987; Contratti Collettivi Nazionali e Contratti Integrativi del Comparto Ministeri e della separata area della Dirigenza amministrativa.

- ***Norme per il personale delle*** **istituzioni** ***scolastiche****:* D.Lgs. 16 aprile 1994, n. 297; Legge 3 maggio 1999, n. 124; Legge 28 marzo 2003, n. 53; Legge 18 luglio 2003, n. 186; Decreto Legislativo 19 febbraio 2004, n.59; Legge 6 giugno 2004, n. 143; Contratti Collettivi Nazionali e Integrativi del Comparto Scuola e della separata area della Dirigenza scolastica, Legge 28 febbraio 1990, n.. 37; Legge 23 dicembre 1998 n. 448, art. 26, commi 8, 9 e 10; D.P.R. 6. marzo 2001, n.190; Legge 27 dicembre 2002, n. 289 art. 35; D.lgs. 17 ottobre 2005, n. 227;

- ***Norme per il personale IRR.E:*** D.P.R. 6 marzo 2001, n. 190.

Tipi di dati trattati

• CONVINZIONI |X| religiose | | filosofiche | | d'altro genere

• CONVINZIONI |X| sindacali

• STATO DI SALUTE |X| patologie attuali |X| patologie pregresse

|X| terapie in corso |X| dati sulla salute relativi anche ai familiari

• VITA SESSUALE | | **(**solo in caso di rettificazione di attribuzione di sesso)

• DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e, del Codice) |X|

OPERAZIONI ESEGUITE

Particolari forme di trattamento

- Interconnessioni *e* raffronti di dati con altro titolare;

- Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;

- Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;

- Organi preposti al riconoscimento della causa di servizio/equo indennizzo, ai sensi del DPR 461/2001;

- Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (d.lgs. n. 626/1994);

- Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro del D.P.R. n. 1124/1965;

- Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della L. 68/1999;

- Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;

-Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;

- Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai Sensi dellaL. 18luglio 2003, n. 186;

-Organi di controllo (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex legge n.20/94 e D.P.R. 20 febbraio 1998, n.38;

- Agenzia delle Entrate: ai fini degli obblighi fiscali del personale ex legge 30 dicembre 1991, n. 413; MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335;

- Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art. 50, comma 3, d.lgs n. 165/2001)

Altre tipologie di trattamenti

• RACCOLTA:	|X| presso gli interessati	|X| presso terzi
• ELABORAZIONE:	|X| in forma cartacea	|X| con modalità informatizzate

Altre operazioni ordinarie:
registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA B

La *"scheda"* individua il trattamento dei dati sensibili e giudiziari concernente tutte le attività relative alla difesa in giudizio del MPI e delle istituzioni scolastiche nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili.

Indicazione del trattamento e descrizione riassuntiva del contesto

Gestione del contenzioso e procedimenti discìplinari

Il trattamento dei dati sensibí1i e giudiziari concerne tutte le attività relative alla difesa in giudizio del Ministero dell'istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari pena1ì e civili.

Finalità di rilevante interesse pubblico perseguite

- **ART. 112:** *"instaurazione e gestione da parte **dei** soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale **o** temporaneo, e di altre forme di impiego che non comportano la **costituzione di un** rapporto di lavoro subordinato"*

- **ART. 67:** *"attività di controllo e ispettive";*

- **ART 68:** " *applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;*

- **ART. 71:** *"attività sanzionatorie e di tutela";*

Fonti normative

- ***Norme comuni:*** Codice Civile; Codice Penale; Codice di Procedura Civile; Codice di Procedura Penale; D.P.R. 10 gennaio 1957, n. 3; D.P.R. 24/11/1971, n. 1199; Legge 6/12/1971, n. 1034; Legge 15/03/1997, n. 59; Legge 21/07/2000, n. 205; D.lgs. 28/08/2000, n. 274; Legge 27/03/2001, n. 97; D.lgs. 30/03/2001, n. 165; Accordi quadro.

- ***Norme relative al personale amministrativo del Ministero dell'Istruzione:*** Contratti Collettivi Nazionali e Contratti Integrativi del Comparto Ministeri e della separata area della Dirigenza amministrativa.

- ***Norme per il personale delle*** **istituzioni** ***scolastiche e degli IRRE****:* D.Lgs. 16 aprile 1994, n. 297; D.P.R. 6. marzo 2001, n.190; Contratti Collettivi Nazionali e Integrativi del Comparto Scuola e della separata area della Dirigenza scolastica;

Tipi di dati trattati

• ORIGINE	|X| razziale	| X | etnica	
• CONVINZIONI	|X| religiose	|X| filosofiche	|X| d'altro genere
• CONVINZIONI	|X| politiche	|X| sindacali	
• STATO DI SALUTE	|X| patologie attuali	|X| patologie pregresse	
	|X| terapie in corso	|X| dati sulla salute relativi anche ai familiari	
• VITA SESSUALE	| X |		

• DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e, del Codice) |X|

OPERAZIONI ESEGUITE

Particolari forme di trattamento

- Comunicazione con altri soggetti pubblici o privati:

- Ministero del Lavoro e delle Politiche Sociali: per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi a Collegi di conciliazione ex D.lgs. 30/03/2001, n. 165;

- Organi arbitrali: per lo svolgimento delle procedure arbitrali ai sensi dei CCNL di settore;

- Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di giustizia;

-Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria: per l'esercizio dell'azione di giustizia;

- Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

Altre tipologie di trattamenti

• RACCOLTA:	|X| presso gli interessati	|X| presso terzi
• ELABORAZIONE:	|X| in forma cartacea	|X| con modalità informatizzate

Altre operazioni ordinarie:

- registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA C

La *"scheda"* individua il trattamento e la descrizione dei dati sensibili nello ambito degli organismi collegiali e delle commissioni istituzionali, organi rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, che delle famiglie e delle associazioni sindacali. Il dato sensibile trattato è quello dell'appartenenza alle organizzazioni sindacali, con riferimento agli organismi o comitati che richiedano la partecipazione di rappresentanti delle organizzazioni sindacali.

Indicazione del trattamento e descrizione riassuntiva del contesto

Organismi Collegiali e Commissioni Istituzionali

Il trattamento dei dati sensibi1i è necessario per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero Istruzione e dell'Ordinamento Scolastico. Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, delle famiglie e delle associazioni sindacali. Il dato sensibile trattato è quello dell'appartenenza alle organizzazioni sindacali, con riferimento agli organismi o comitati che richiedano la partecipazione di rappresentanti delle organizzazioni sindacali.

Finalità di rilevante interesse pubblico perseguite

- **ART. 65:** *"pubblicità dell'attività di organi";*
- **ART. 95:** *"dati sensibili e giudiziari relativi alle finalità di istruzione e di formazione in ambito scolastico, professionale, superiore o universitario".*

Fonti normative

- ***Norme comuni:*** D.Lgs. 16 aprile 1994, n. 297; Contratti Collettivi Nazionali e Integrativi di Comparto.

Tipi di dati trattati

• ORIGINE	| | razziale	| | etnica		
• CONVINZIONI	| | religiose	| | filosofiche	| | d'altro genere	
• CONVINZIONI	| | politiche	|X| sindacali		
• STATO DI SALUTE	| | patologie attuali	| | patologie pregresse		
	| | terapie in corso	| | dati sulla salute relativi anche ai familiari		
• VITA SESSUALE	| |			

• DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e, del Codice) |X|

Altre tipologie di trattamenti

• RACCOLTA:	|X| presso gli interessati	|X| presso terzi
• ELABORAZIONE:	|X| in forma cartacea	|X| con modalità informatizzate

Altre operazioni ordinarie:

- registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA D

La *"scheda"* individua il trattamento di tutti i dati coinvolti nelle attività propedeutiche all'avvio dell'anno scolastico: si tratta dei dati forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio di ogni ordine e grado re *(è possibile, in tal caso, imbattersi in dati relativi alle origini razziali ed etniche, alle convinzioni religiose, allo stato di salute, alle vicende giudiziarie*).

Indicazione del trattamento e descrizione riassuntiva del contesto

Attività propedeutiche all'avvio dell'anno scolastico

I dati sono forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio nelle istituzioni scolastiche di ogni ordine e grado ivi compresi convitti, educandati e scuole speciali. Nell'espletamento delle attività propedeutiche all'avvio dell'anno scolastico da parte delle istituzioni scolastiche, possono essere trattati dati sensibili relativi:
*alle **origini razziali ed etniche,** per favorire l'integrazione degli alunni con cittadinanza non italiana;*
*alle **convinzioni religiose**, per garantire la libertà di credo religioso e per la fruizione all'insegnamento della religione cattolica o delle attività alternative a tale insegnamento;*
*allo **stato di salute**, per assicurare l'erogazione del sostegno agli alunni disabili e per la composizione delle classi;*
*alle **vicende giudiziarie**,per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione; i dati giudiziari emergono anche nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno nonché nei confronti degli alunni che abbiano commesso reati.*

Finalità di rilevante interesse pubblico perseguite

Le finalità di cui agli artt. 68, 73, 86, 95 del D.lgs. 30giugno 2003, n. 196.

Fonti normative

Leggi regionali sul diritto allo studio ai sensi del D.P.R. 24/07/1977, n.616; Legge 25/03/1985, n.121; Legge 5/02/1992, n. 104; D.lgs. 16/04/94,n.297; Legge 24/06/1997, n.196; D.lgs. 31/03/1998, n.112; D.P.R. 24/06/1998, n.249; D.P.R. 08/03/1999, n.275; D.P.R. 31/08/1999, n. 394; Legge 10/03/2000, n.62; Legge 28/03/2003, n. 53; D.lgs. 19/02/2004, n.59; D.lgs. 15/04/2005, n. 76; D.lgs. 17/10/2005, n.226.

Tipi di dati trattati

• ORIGINE	| X | razziale	| X | etnica	
• CONVINZIONI	| X | religiose	| filosofiche	| X | d'altro genere
• CONVINZIONI	| politiche	| sindacali	
• STATO DI SALUTE	| X | patologie attuali	| X | patologie pregresse	
	| X | terapie in corso	| X | dati sulla salute relativi anche ai familiari	
• VITA SESSUALE	|		

• DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e, del Codice) |X|

OPERAZIONI ESEGUITE

Particolari forme di trattamento

- Comunicazione ai seguenti soggetti per le seguenti finalità:

- agli Enti Locali per la fornitura dei servizi ai sensi del D.lgs. 31/03/1998, n.112, limitatamente ai dati indispensabili all'erogazione del servizio;
- ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica ai sensi delle leggi regionali sul diritto allo studio limitatamente ai dati indispensabili all'erogazione del servizio;
- alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di lavoro Handicap di Istituto e per la predisposizione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 05/02/1992, n. 104.

Altre tipologie di trattamenti

• RACCOLTA:	|X| presso gli interessati	|X| presso terzi
• ELABORAZIONE:	|X| in forma cartacea	|X| con modalità informatizzate

Altre operazioni ordinarie:

- registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA E

La *"scheda"* attiene al rilevamento e alla trattazione di dati raccolti nell'ambito dell'attività educativa, didattica e formativa e di valutazione (*anche in tal caso possono rilevare i dati sensibili relativi alle origini razziali ed etniche, alle convinzioni religiose, allo stato di salute, ai dati giudiziari, alle convinzioni politiche - per la costituzione e il funzionamento delle Consulte degli studenti*).

Indicazione del trattamento e descrizione riassuntiva del contesto

Attività educativa, didattica, formativa, di valutazione

Nell'espletamento delle attività educative, didattiche e formative, curricolari ed extracurricolari, di valutazione ed orientamento, di scrutini ed esami, da parte delle Istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali, possono essere trattati dati sensibili relativi:
*alle **origini razziali ed etniche,** per favorire l'integrazione degli alunni con cittadinanza non italiana;*
*alle **convinzioni religiose**, per garantire la libertà di credo religioso;*
*allo **stato di salute**, per assicurare l'erogazione del servizio di refezione scolastica, del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate e ai viaggi di istruzione;*
*ai **dati giudiziari,** per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione;*
*alle **convinzioni politiche,** per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei genitori.*
I dati sensibili possono essere trattati per le operazioni di valutazione periodica e finale, per le attività di orientamento e per la compilazione della certificazione delle competenze.

Finalità di rilevante interesse pubblico perseguite

Le finalità di cui agli artt. 68, 73, 86, 95 del D.lgs. 30giugno 2003, n. 196.

Fonti normative

Leggi regionali sul diritto allo studio ai sensi del D.P.R. 24/07/1977, n.616; Legge 25/03/1985, n.121; Legge 5/02/1992, n. 104; D.lgs. 16/04/94, n.297; D.P.R. 10/10/1986, n. 567; Legge 24/06/1997, n.196; D.lgs. 31/03/1998, n.112; D.P.R. 24/06/1998, n.249; D.P.R. 08/03/1999, n.275; D.P.R. 31/08/1999, n. 394; Legge 10/03/2000, n.62; Legge 28/03/2003, n. 53; D.lgs. 19/02/2004, n.59; D.lgs. 15/04/2005, n. 76; D.lgs. 21/04/2005, n. 77; D.lgs. 17/10/2005, n.226; D.P.R. 23/12/2005, n. 301.

Tipi di dati trattati

• ORIGINE | X | razziale | X | etnica

• CONVINZIONI | X | religiose | X| filosofiche | X | d'altro genere

• CONVINZIONI | X | politiche | | sindacali

• STATO DI SALUTE | X | patologie attuali | X | patologie pregresse

| X | terapie in corso | X | dati sulla salute relativi anche ai familiari

• VITA SESSUALE | X |

• DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e, del Codice) |X|

OPERAZIONI ESEGUITE

Particolari forme di trattamento

- Comunicazione ai seguenti soggetti per le seguenti finalità:
  a) Alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente la carriera scolastica degli alunni, 1imitatamente ai dati indispensabili all'erogazione del servizio;
  b) agli Enti Locali per la fornitura dei servizi ai sensi del D.lgs. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;
  c) ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto alla attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
  d) agli Istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;
  e) all'INAIL per la denuncia di infortuni ex - D.P.R. 30 giugno 1965, n. 1124;
  f) alle AUSL e agli Enti Locali per il funzionamento dei gruppi di Lavoro di istituto per l'Handicap e per la predisposizione e la verifica Piano Educativo Individuale, ai sensi della Legge 5 febbraio 1992, n. 104;
  g) ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro, ai sensi della 24 giugno 1997, n. 196 e del D. Lgs.

21/04/2005, n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio.
Altre tipologie di trattamenti
• RACCOLTA: |X| presso gli interessati |X| presso terzi • ELABORAZIONE: |X| in forma cartacea |X| con modalità informatizzate Altre operazioni ordinarie: • registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, raffronto, utilizzo, blocco, cancellazione e distruzione.

SCHEDA F

La *"scheda"* individua i dati sensibili e giudiziari concernenti le attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti disciplinari etc.) con gli alunni e con le famiglie.

Indicazione del trattamento e descrizione riassuntiva del contesto
Rapporti scuola-famiglie: gestione del contenzioso *Il trattamento di dati sensibili e giudiziari concerne tutte le attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, ecc.)con gli alunni e con le famiglie, e tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.*
Finalità di rilevante interesse pubblico perseguite
Le finalità di cui agli artt. 67 e 71 del D.lgs. 30giugno 2003, n. 196.
Fonti normative
Codice Civile; Codice Penale; Codice di Procedura Civile; Codice di procedura Penale; D.P.R. 24/11/1971, n. 1199; D.lgs. 16/04/94, n.297; D.P.R. 24/06/1998, n.249; D.P.R. 08/03/1999, n.275; Legge 28/03/2003, n. 53; D.lgs. 19/02/2004, n. 59; D.lgs. 21/04/2005, n. 76; D.lgs.

21/04/2005, n. 77; D.lgs. 17/10/2005, n.226.

Tipi di dati trattati

• ORIGINE | X | razziale | X | etnica

• CONVINZIONI | X | religiose | X| filosofiche | X | d'altro genere

• CONVINZIONI | X | politiche | X | sindacali

• STATO DI SALUTE | X | patologie attuali | X | patologie pregresse

| X | terapie in corso | X | dati sulla salute relativi anche ai familiari

• VITA SESSUALE | X |

• DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e, del Codice) |X|

OPERAZIONI ESEGUITE

Particolari forme di trattamento

- Comunicazione con altri soggetti pubblici e privati:
  a) Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia;
  b) Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia;
  c) Liberi professionisti, ai fini di patrocinio o di consulenza compresi quelli di controparte per le finalità di corrispondenza.

Altre tipologie di trattamenti

• RACCOLTA: |X| presso gli interessati |X| presso terzi

• ELABORAZIONE: |X| in forma cartacea |X| con modalità informatizzate

Altre operazioni ordinarie:

- registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

Misure minime organizzative adottate

dall'Istituzione scolastica

"Garibaldi-Capuana" di Raffadali, in materia di TRATTAMENTO E GESTIONE DEI DATI PERSONALI

a.s. 2017-18

Articolo 1

Oggetto e ambito di applicazione

1. Il presente regolamento disciplina le modalità di trattamento dei dati personali, in formato cartaceo e elettronico, da parte dell'Istituzione Scolastica **"Garibaldi-Capuana" di Raffadali (AG).**
2. Per dato personale si intende qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
3. Per dato sensibile si intende qualsiasi dato personale idoneo a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
4. Per dato giudiziario si intende qualsiasi dato personale idoneo a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Articolo 2

Principi di carattere generale

1. I trattamenti di dati personali effettuati all'interno dell'Istituzione Scolastica devono avvenire secondo le modalità definite dalla normativa in vigore, con particolare riguardo a quanto disposto dal Dlgs 196/2003 e dalla normativa collegata.
2. Occorre custodire e controllare i dati personali oggetto del trattamento per contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dai casi consentiti o altrimenti trattati in modo illecito.
3. Chiunque, all'interno di questa istituzione scolastica, tratti dati personali, è tenuto all'obbligo della dovuta riservatezza in ordine alle informazioni delle quali sia venuto a conoscenza.
4. L'obbligo di mantenere la dovuta riservatezza, in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, permane anche quando sia venuto meno l'incarico stesso.

5. Tutti i trattamenti dei dati personali vanno necessariamente organizzati secondo una procedura che garantisca: una continua e idonea custodia dei dati oggetto del trattamento; un adeguato controllo sugli accessi non autorizzati ai dati; il maggior livello possibile di sicurezza in merito alla conservazione dei dati.
6. Il trattamento dei dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali della scuola. Al di fuori delle finalità strettamente istituzionali, dentro la scuola non si possono trattare dati personali né su supporto cartaceo né su supporto elettronico.
7. I dati personali oggetto dei trattamenti devono essere esatti ed aggiornati, inoltre devono essere pertinenti rispetto alle finalità del trattamento, completi e non eccedenti le finalità per le quali vengono raccolti e trattati. Ne consegue che i trattamenti dei dati vanno ridotti a quanto indispensabile rispetto alle finalità istituzionali perseguite.
8. Nell'ambito delle indicazioni del presente Regolamento, particolare attenzione va prestata al trattamento di dati sensibili e giudiziari.
9. L'istituto esegue verifiche periodiche sull'attualità degli incarichi affidati in merito al trattamento dei dati, nonché sull'esattezza e l'aggiornamento dei dati sensibili e giudiziari, sulla loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite.

Articolo 3

Accesso ai luoghi in cui si effettuano i trattamenti

1. L'accesso ai locali in cui si trovano le apparecchiature informatiche dell'istituzione scolastica (server di rete, computer, stampanti, ecc) utilizzati per il trattamento dei dati personali, nonché gli archivi e i registri cartacei contenenti dati personali, è controllato ed è permesso esclusivamente al personale debitamente incaricato e autorizzato.
2. I locali ad accesso controllato sono chiusi anche se presidiati. Dopo l'uscita dell'ultimo incaricato/addetto al trattamento dei dati i locali sono chiusi a chiave.
3. L'elenco delle persone autorizzate ad accedere ai locali di cui al presente articolo è periodicamente verificato dal responsabile del trattamento o da un suo delegato.
4. Eventuali visitatori occasionali delle aree ad accesso controllato sono previamente autorizzati dal Responsabile del trattamento dei dati e accompagnati da un incaricato, che controllerà che i visitatori non accedano a dati in possesso dell'istituzione scolastica se non previamente autorizzati e incaricati.
5. L'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo in seguito ad apposita autorizzazione del Dirigente scolastico.

Articolo 4

Raccolta, Comunicazione e diffusione dei dati

1. E' vietata ogni forma di diffusione e comunicazione dei dati personali a terzi soggetti, a meno che ciò non sia previsto da Legge o da Regolamento e autorizzato dal titolare del trattamento dei dati personali.

2. I dati idonei a rivelare lo stato di salute non possono essere diffusi.
3. E' necessario consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente l'informativa.
4. Le comunicazioni di dati agli interessati (persone fisiche e giuridiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata; se effettuate per iscritto dovranno essere consegnate in contenitori chiusi.

Articolo 5

Tenuta dei registri e degli archivi cartacei

1. I dati personali trattati attraverso supporto cartaceo possono essere trattati solo da personale debitamente incaricato e nel rispetto delle disposizioni contenute nelle lettere d'incarico e nel presente regolamento.
2. I registri di classe, contenenti dati personali, durante l'orario delle lezioni devono essere tenuti in classe sulla scrivania e affidati all'insegnante di turno. Al termine delle lezioni vengono depositati dall'insegnante dell'ultima ora di lezione negli appositi armadietti chiusi a chiave e conservati per essere riconsegnati da un collaboratore scolastico, incaricato del trattamento, all'inizio delle lezioni.
3. I certificati medici ricevuti vanno consegnati al più presto in Segreteria;
4. Durante l'orario di servizio il docente è responsabile della custodia e della conservazione dei registri personali e dei registri di valutazione attraverso cui sono trattati dati personali. Fuori dall'orario di servizio il registro viene conservato negli appositi armadietti chiusi a chiave.
5. E' fatto divieto di fotocopiare/scannerizzare documenti contenenti dati sensibili senza l'autorizzazione del responsabile o del titolare del trattamento;
6. E' fatto divieto di esportare documenti o copie contenenti dati personali, all'esterno dell'Istituto, senza l'autorizzazione del titolare o del responsabile del trattamento; tale divieto si estende anche all'esportazione telematica;
7. I dati comuni sono custoditi separati dai dati sensibili in sottofascicoli chiusi con dicitura “riservato”;
8. I documenti contenenti dati sensibili e giudiziari sono custoditi in armadi e/o cassetti chiusi a chiave.

Articolo 6

Trattamenti in formato elettronico – Principi generali

1. Le principali misure di sicurezza relative ai trattamenti di dati in formato elettronico sono indicate nel Documento Programmatico sulla Sicurezza della presente Istituzione Scolastica;
2. L'utilizzo dei Personal Computer e della Rete interna è permesso esclusivamente per lo svolgimento delle attività istituzionali della scuola;
3. La scuola adotta procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

4. I computer della Segreteria devono essere connessi ad un segmento della rete locale non visibile o raggiungibile da altri computer dell'istituto;
5. La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

Articolo 7

Trattamenti in formato elettronico – Regole operative

1. E' fatto divieto, agli utilizzatori di strumenti elettronici, di lasciare incustodito, o accessibile lo strumento elettronico stesso; in particolare, in caso di allontanamento anche temporaneo dal posto di lavoro, è vietato lasciare aperto il proprio sistema operativo con la password inserita, a meno che il sistema non richieda automaticamente la password in caso di inattività per un tempo superiore a 3 minuti.
2. L'accesso ai dati trattati elettronicamente da parte degli incaricati e degli addetti esterni alla manutenzione è possibile solo in seguito ad autorizzazione scritta.
3. La manutenzione degli elaboratori, che preveda o meno il trasferimento fisico presso un laboratorio di riparazioni, è autorizzata solo a condizione che il fornitore del servizio si impegni al rispetto della normativa sulla protezione dei dati personali; il fornitore si deve altresì impegnare a mantenere la dovuta riservatezza in ordine ai dati di cui sia venuto a conoscenza e a non utilizzarli fuori dai casi consentiti.
4. Tutte le operazioni di manutenzione che sono effettuate all'interno dell'Istituzione Scolastica avvengono con la supervisione del Responsabile del trattamento o di un suo delegato.
5. Gli hard disk non sono condivisi in rete se non in casi specifici e limitati;
6. E' fatto assoluto divieto di memorizzare, sulla propria postazione di lavoro, dati di carattere personale che non siano inerenti alla funzione svolta.
7. E' proibito installare qualsiasi programma da parte dell'utente o di altri operatori, a meno che non siano autorizzati dell'amministratore del sistema.
8. E' vietato fare uso delle funzionalità di accesso remoto del proprio computer se non espressamente autorizzati dall'Amministratore del sistema.
9. All'uso di supporti rimovibili (floppy, cd, zip) va sempre preferito l'utilizzo di internet o di un file server locale.
10. Va evitato l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza.
11. E' fatto divieto di “scaricare“ dalla rete internet ogni sorta di file, eseguibile e non; La decisione di “scaricare” può essere presa solo dal responsabile del trattamento o dall'amministratore del sistema (se nominato).
12. Va attivata la protezione massima per gli utenti del programmi di posta utilizzati, al fine di proteggersi dal codice html di certi messaggi e-mail, dato che alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer.
13. E' fatto divieto di utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi dello Stato.

14. Gli allegati di posta, se non si è certi della loro provenienza, non vanno aperti e in ogni caso vanno analizzati con un antivirus.
15. E' opportuno impostare l'antivirus anche nella funzione di autoriparazione.
16. Avvisare sempre l'amministratore di sistema nel caso in cui il processo di autoriparazione non vada a buon fine.
17. E' opportuno conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge.
18. Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino anomalie di funzionamento quali ad esempio modifica e sparizione di dati, irregolarità nell'utilizzo del Computer.

Articolo 8

Disposizioni in merito alla gestione delle password

1. Tutti gli incaricati del trattamento dei dati personali accedono agli strumenti elettronici usati per i trattamenti attraverso un codice identificativo personale (in seguito indicato user-id) e password personale;
2. User-id e password iniziali sono assegnati dal Responsabile del trattamento o dal custode delle password, se necessario con il supporto dell' Amministratore di sistema.
3. I codici assegnati sono segreti, non possono essere assegnati né comunicati ad altri soggetti; vanno custoditi con diligenza e riservatezza;
4. L'user-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome;
5. La password è composta da almeno 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'Istituzione scolastica, al suo utilizzatore o al suo ufficio;
6. La password deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato;
7. Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima;
8. Le password verranno prontamente disattivate dopo tre mesi di non utilizzo;
9. In caso di necessità, il Responsabile del trattamento o l'amministratore di sistema è autorizzato a intervenire sui personal computer;
10. L'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse che altri non autorizzati ne sono venuti a conoscenza.

Articolo 9

Sanzioni

1. In caso di violazione delle disposizioni del presente regolamento, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dal regolamento d'istituto.

Il Responsabile del Trattamento
(Ins. Gerlando Alonge)

Il Titolare del Trattamento
(Dott. Silvana Spirio)

Il Dirigente Scolastico
(Dott. SILVANA SPIRIO)

Misure minime ICT adottate dall'Istituzione scolastica

Ai sensi della Direttiva PCM del 01/08/2015 e della CIRCOLARE 18 aprile 2017 , n. 2/2017

PREMESSA

Il presente documento è emesso in attuazione della Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015 e contiene le *Misure minime di sicurezza ICT per le Pubbliche Amministrazioni* le quali costituiscono parte integrante delle *Linee Guida per la sicurezza ICT delle Pubbliche Amministrazioni*.

Le Misure minime ICT per la PA sono un insieme ordinato e ragionato di "controlli", ossia azioni puntuali di natura tecnica od organizzativa, che l'Agenzia per l'Italia Digitale ha predisposto al fine di fornire alle pubbliche amministrazioni un riferimento pratico per valutare e innalzare il proprio livello di sicurezza informatica, avvalendosi in ciò della sua facoltà di dettare "indirizzi, regole tecniche e linee guida in materia di sicurezza informatica" anche in ottemperanza alla direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri che impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici.

Come ben specifica la Premessa presente nel documento, l'insieme dei controlli che costituiscono le Misure Minime AgID, denominati AgID Basic Security Controls (ABSC) è stato composto partendo dalla base, già consolidata e assai apprezzata dalla comunità mondiale degli esperti di sicurezza, costituita dai cosiddetti "SANS 20" (oggi noti come Critical Security Controls) emessi dal SANS Institute. Tuttavia gli ABSC non sono una mera e letterale traduzione italiana dei controlli SANS/CSC, ma costituiscono un ragionato adattamento alla nostra realtà nazionale di alcuni controlli accuratamente selezionati come maggiormente significativi tra quelli presenti nelle ultime due versioni (la 5.1 e la 6.0) della lista. Ciò in considerazione delle peculiarità

della nostra Pubblica Amministrazione, che non trova immediato riscontro nella più evoluta realtà statunitense.

Massima cura è stata, inoltre, posta nel modulare i controlli in modo da non costringere le Amministrazioni, soprattutto quelle più piccole, ad introdurre misure esagerate per la propria organizzazione, con evidente inutile dispendio di risorse.

Per facilitarne l'adozione, minimizzando gli impatti implementativi sull'organizzazione interessata, **i controlli sono inoltre stati suddivisi in tre gruppi verticali**, riferiti a livelli complessivi di sicurezza crescente. I controlli del primo gruppo (**livello "Minimo"**) sono quelli strettamente obbligatori ai quali ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve essere conforme in termini tecnologici, organizzativi e procedurali: essi dunque rappresentano complessivamente il livello sotto al quale nessuna Amministrazione può scendere.

I controlli del secondo gruppo (**livello "Standard"**) rappresentano la base di riferimento per la maggior parte delle Amministrazioni, e costituiscono un ragionevole compromesso fra efficacia delle misure preventive ed onerosità della loro implementazione.

I controlli del terzo gruppo (**livello "Alto"**) rappresentano infine il livello adeguato per le organizzazioni maggiormente esposte a rischi, ad esempio per la criticità delle informazioni trattate o dei servizi erogati, ma anche l'obiettivo ideale cui tutte le altre organizzazioni dovrebbero tendere. Naturalmente va considerato che il raggiungimento di elevati livelli di sicurezza, quando sono molto elevati sia la complessità della struttura che l'eterogeneità dei servizi da essa erogati, può essere eccessivamente oneroso se applicato in modo generalizzato: ogni Amministrazione dovrà pertanto avere cura di individuare al suo interno gli eventuali sottoinsiemi tecnici e/o organizzativi, caratterizzati da una sostanziale omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi.

Per quanto riguarda i contenuti, le Misure Minime prevedono, nella loro formulazione attuale, otto insiemi (o "classi") di controlli.

I controlli delle prime due classi (**ABSC 1 e 2**) riguardano rispettivamente l'inventario dei dispositivi autorizzati e non autorizzati e quello dei software autorizzati e non autorizzati. In pratica essi impongono all'organizzazione di gestire attivamente i dispositivi hardware e i pacchetti software in uso, predisponendo e mantenendo aggiornati, a diversi livelli di dettaglio e con differenti modalità attuative a seconda del livello di sicurezza, i rispettivi inventari, e prevedendo inoltre meccanismi per individuare e/o impedire tutte le anomalie operative, ossia l'impiego di elementi non noti e/o esplicitamente autorizzati.

I controlli della terza classe (**ABSC 3**) riguardano la protezione delle configurazioni hardware e software sui sistemi in uso presso l'organizzazione.

I controlli della quarta classe (**ABSC 4**) sono finalizzati ad individuare tempestivamente, e correggere, le vulnerabilità dei sistemi in uso, minimizzando la finestra temporale nella quale le vulnerabilità presenti possono essere sfruttate per condurre attacchi contro l'organizzazione.

I controlli della quinta classe (**ABSC 5**) sono rivolti alla gestione degli utenti, in particolare gli amministratori, ed hanno lo scopo di assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi sui sistemi in uso.
I controlli della sesta classe (**ABSC 8**) hanno lo scopo di contrastare l'ingresso e la diffusione nell'organizzazione di codice malevolo di qualsiasi provenienza.

I controlli della settima classe (**ABSC 10**) sono relativi alla gestione delle copie di sicurezza delle informazioni critiche dell'organizzazione, che in ultima analisi sono l'unico strumento che garantisce il ripristino dopo un incidente.

L'ottava ed ultima classe (**ABSC 13**) riguarda infine la protezione contro l'esfiltrazione dei dati dell'organizzazione, in considerazione del fatto che l'obiettivo principale degli attacchi più gravi è la sottrazione di informazioni.
La norma attuativa prevede che ciascuna Amministrazione debba non solo implementare i controlli rilevanti, ma anche dare brevemente conto della modalità di implementazione compilando appositi moduli di implementazione che dovranno essere firmati digitalmente con marcatura temporale. Dopo la sottoscrizione, il presente documento deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso.

Moduli di implementazione delle misure minime ICT
ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Esiste un inventario informatizzato
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Si, le macchine possono essere collegate solo previa registrazione di MAC e IP in inventario
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Si, le macchine possono essere collegate solo previa registrazione di MAC e IP in inventario
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	L'installazione di software è bloccata per tutti gli utenti. Eventuali nuovi software sono installati esclusivamente dall'amministratore dopo verifica della tipologia e della funzionalità.
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Tutti i dispositivi sono protetti con antivirus e software che rimuovono automaticamente eventuali installazioni non autorizzate (DeepFreeze)
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Tutte le macchine sono protette da password e hanno un antivirus installato. Gli utenti non hanno privilegi di amministratore.
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Le macchine omogenee per tipo e sistema operativo hanno delle configurazioni standardizzate.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Il sistema DeepFreeze provvede automaticamente al ripristino della configurazione in caso di alterazioni
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Sono conservate su DVD
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Le operazioni di amministrazione da remoto sono impedite. In caso di necessità vengono abilitate temporaneamente connessioni attraverso protocolli sicuri e disabilitate al termine dell'intervento.
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file	

				deve essere generato un alert.	
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	In caso di modifiche si procede alla riconfigurazione dei firewall e ad una scansione completa dei sistemi
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a	

				tale interfaccia e la utilizzi propriamente.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Gli antivirus sono configurati per l'aggiornamento automatico
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	I dispositivi sono configurati per l'aggiornamento automatico del SO
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non vi sono sistemi separati dalla rete.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Esistono procedure automatizzate di backup per la salvaguardia dei dati residenti in sede.
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Tutte le patch relative a vulnerabilità vengono immediatamente implementate appena disponibili
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID	Livello	Descrizione	Modalità di implementazione

5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Sono identificati tra il personale n° 2 tecnici specializzati per le attività di amministrazione.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	L'accesso alle utenze amministrative è limitato al minimo indispensabile. È in via di estensione una procedura di registrazione degli accessi.
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'inventario è presente.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Le credenziali vengono sostituite prima dell'allacciamento in rete.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Le password devono includere lettere maiuscole e minuscole,caratteri speciali e numeri.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Per le password viene imposta una scadenza trimestrale o semestrale in funzione del grado di criticità.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Non è possibile riutilizzare password precedentemente utilizzate.

5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	La distinzione è assicurata nella configurazione del server
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Sono associate a nome e cognome degli utenti ad ogni credenziale di accesso.
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Le credenziali sono disponibili solo per i tecnici autorizzati.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	L’elenco cartaceo delle PWD è custodito in cassaforte ed accessibili solo al responsabile della struttura ed al direttore sga.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizzano

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	SI
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Si
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad	

				un repository centrale (syslog) dove sono stabilmente archiviati.	
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	La rete “Pubblica” poggia su una linea dati indipendente da quelle degli uffici e dei laboratori
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Si
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Si
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Si
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Si
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Si
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario,	Si

				prevedendo anche l'impiego di strumenti antispam.	
8	9	2	M	Filtrare il contenuto del traffico web.	Si
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Si
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Il backup è effettuato due volte al giorno
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Le copie sono cifrate
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	Le copie vengono duplicate su dispositivi rimuovibili

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	L'analisi è in via di implementazione. Si stà procedendo al trasferimento su servizi cloud garantiti dai fornitori di servizi (ARGO) È stata richiesta ai fornitori la

					dichiarazione relativa alle misure implementate
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	La misura è implementata nel firewall
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	

Oggetto: nomina incaricati del trattamento di dati personali – unità organizzativa "Segreteria", ai sensi del D.Lgs. n. 196/2003 (Codice della Privacy).-

IL DIRIGENTE SCOLASTICO

nella qualità di Titolare del trattamento dei dati personali

- **Visto** il D.Lgs 196/2003 "Codice in materia di protezione dei dati personali", che d'ora in poi, nel presente documento sarà richiamato semplicemente come "Codice";

- **Premesso che**
  - ai sensi dell'art. 28 del Codice nel presente atto, il Titolare dei dati personali trattati da parte di questo Istituto è l'Istituto stesso, di cui il Dirigente scolastico pro-tempore è il Legale Rappresentante;
  - il Titolare ha applicato l'art. 29 del Codice, che consente la facoltà di nominare uno o più Responsabili di tutti o parte dei trattamenti e che, pertanto, a tale scopo è stato nominato L'ins. Gerlando Alonge (Docente Interno) tel. 3885879669.
  - risulta vigente la facoltà di nominare il Responsabile di tutti i trattamenti e di delegarlo nei compiti di nomina degli Incaricati;
  - l'art. 30 del Codice impone di nominare gli Incaricati del trattamento dei dati personali;
  - l'art. 33 del medesimo testo normativo impone di adottare le misure di sicurezza disposte dal Codice e almeno le misure minime individuate dall'allegato B del Codice stesso;

- **Considerato che**
  - occorre definire le misure minime di sicurezza per l'attività di ciascuna unità organizzativa nel trattamento di dati personali e per l'esecuzione dei procedimenti amministrativi;
  - bisogna individuare gli Incaricati al trattamento dei dati e che la nomina a Incaricato non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate per ragioni d'ufficio, ma provvede a regolarizzare con una specifica autorizzazione agli Incaricati il trattamento dei dati personali mediante apposite istruzioni sulle modalità cui attenersi nel trattamento degli stessi;
  - l'articolazione organizzativa dell'Istituto è fondata su diverse tipologie di personale: collaboratori del Dirigente scolastico, personale docente (compresi docenti esterni ufficialmente incaricati di esami o altre funzioni presso l'Istituto), personale amministrativo, personale ausiliario (Collaboratori scolastici) e componenti (anche esterni alla scuola) degli Organi Collegiali;

D E C R E T A

1) di designare **l'unità organizzativa "segreteria" ,** comprendente i dipendenti aventi il profilo di Assistenti Amministrativi e di DSGA (Direttore dei Servizi Generali ed Amministrativi) quali **Incaricati** del trattamento dei **dati personali** di seguito specificati:

a. – Gestione degli Alunni – Dati personali trattati dalla Sig. ra Danile Anna;
b. -Amministrazione del Personale dipendente– Dati personali trattati dalla sig.ra Salemi Angelo
- Collaborazioni professionali – Dati personali trattati dal D.S.G.A Sig.ra Vincenza Faseli;
c. - Acquisti e fornitori – Dati personali trattati dal D.S.G.A Sig.ra Vincenza Faseli;
d. – Contabilita' (Gestione finanziaria e del bilancio) – Dati personali trattati dal D.S.G.A Vincenza Faseli;
e. - Gestione Istituzionale e Protocollo-– Dati personali trattati dal Sig.ra Plano Maria Giovanna;
f. Il D.S.G.A. Sig.ra Vicenza Faseli viene incaricato per il trattamento di tutti i dati personali presenti in Segreteria e per il coordinamento di tutte le attività di segreteria relative alla conservazione e tutela dei dati personali.

2) di dare atto che ogni dipendente che cessa di far parte di questa unità organizzativa cessa automaticamente dalla funzione di Incaricato, mentre ogni nuovo dipendente che entra a far parte di questa unità organizzativa assume automaticamente la funzione di Incaricato, con la conseguenza che in un determinato momento l'elenco degli incaricati appartenenti a questa unità organizzativa corrisponde all'elenco dei dipendenti validamente in servizio che ne fanno parte;
3) di autorizzare questa categoria di Incaricati a trattare tutti i dati personali con cui entrino comunque in contatto nell'ambito dell'espletamento dell'attività di loro competenza o contenuti nelle banche dati, in archivi cartacei

anche frammentari, nelle memorie dei computer, negli archivi dell'intera scuola e dei dati personali comunque raccolti, anche in occasione della sostituzione dei colleghi assenti, assumendo i relativi obblighi al trattamento dei dati affidati al personale che si sostituisce;

4) di autorizzare l'unità organizzativa "Segreteria" a trattare i dati sensibili e giudiziari con cui venga a contatto durante l'attività di competenza nell'ambito dell'Istituto;
5) di indicare per l'unità organizzativa "Segreteria" quali misure di sicurezza da applicare tassativamente nel trattamento dei dati personali in genere, nella gestione di banche dati cartacee, nell'utilizzo dei computer, nelle comunicazioni anche elettroniche;
6) di mettere a disposizione degli incaricati copia del D.Lgs 196/2003 ed altri materiali informativi sulla materia;
7) di organizzare apposite riunioni esplicative e formative, se necessario;
8) di mettere a disposizione, non appena redatto, il Documento Programmatico sulla Sicurezza dei dati personali;
9) di consegnare, all'atto dell'assunzione in servizio, a ogni nuovo componente, anche temporaneo, dell'unità organizzativa in oggetto, copia del presente decreto e i relativi allegati e di incaricare il DGSA di provvedere affinché riceva un'adeguata formazione individuale;
10) di disporre, fermi restando obblighi e responsabilità civili e penali dei dipendenti pubblici nell'ambito delle attività d'ufficio e in relazione ai vincoli disciplinari, l'obbligo tassativo di attenersi alle suddette istruzioni per tutti i dipendenti facenti parte dell'unità organizzativa "Segreteria".

Per il trattamento dei dati di cui ai punti sopraelencati, gli Incaricati devono attenersi alle seguenti Istruzioni generali.

1. **Fonte normativa - Gli Incaricati devono** attenersi rigorosamente a tutte le regole dettate dal D.Lgs n. 196/2003.
2. **Riservatezza -** Gli Incaricati hanno l'obbligo di mantenere il dovuto **riserbo in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico**, che deve permanere **in ogni caso**, anche quando sia venuto meno l'incarico stesso (art.326 del codice penale e art. 28 della legge n. 241/90).
3. **Autorità -** Ai sensi dell'art. 30 del Codice, gli Incaricati del trattamento devono operare sotto la diretta autorità del Titolare (o del Responsabile, se nominato) e devono elaborare i dati personali ai quali hanno accesso, attenendosi alle istruzioni impartite.
4. **Finalità del trattamento -** Ai sensi dell'art. 18 del Codice in materia di protezione dei dati personali, il trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.
5. **Modalità di trattamento dei dati – Il trattamento dei dati** può essere effettuato **manualmente,** mediante **strumenti informatici, telematici o altri supporti.** Ai sensi dell'art. 11 del Codice, il trattamento deve applicare il principio **di pertinenza e non eccedenza** rispetto alle finalità del trattamento medesimo; pertanto è consentita l'acquisizione dei soli dati personali strettamente indispensabili per adempiere alle finalità richieste dall'interessato. Ogni acquisizione di dati dev'essere preceduta dall'apposita informativa all'Interessato, di cui all'art. 13 e 22, avendo cura nel caso di documenti ritenuti potenzialmente classificabili come sensibili o giudiziari, di fare espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento.
6. **Liceità -** I dati devono essere trattati in modo **lecito e secondo correttezza,** devono essere **esatti ed aggiornati.**
7. **Comunicazione -** E' vietata all'Incaricato qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia funzionale allo svolgimento dei compiti affidati. Ai sensi dell'articolo 19 del Codice, la comunicazione da parte della scuola ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma, la comunicazione è ammessa previa richiesta al Garante e attesa del diniego o del silenzio-assenso dopo 45 giorni. La comunicazione da parte della scuola a privati o a enti pubblici economici e la diffusione sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.
8. **Protezione -** Per il trattamento devono essere seguite le norme di legge in materia di tutela della riservatezza dei dati personali e devono essere applicate le misure di protezione previste dal Titolare.
9. **Modalità di trattamento dei dati sensibili/giudiziari:** Ferma restando l'applicazione delle disposizioni vigenti in materia di trattamento dei dati sensibili e giudiziari e delle istruzioni impartite dal Titolare e dal Responsabile del trattamento, i documenti (anche tuttora in lavorazione e non definitivi) ed i supporti recanti dati sensibili o giudiziari devono essere conservati in elementi di arredo muniti di serratura e non devono essere lasciati incustoditi in assenza dell'incaricato.
10. **Trattamenti di dati inerenti la salute:** i supporti ed i documenti recanti dati relativi alla salute e alle abitudini sessuali devono essere conservati separatamente in contenitori muniti di serratura.

ISTRUZIONI AGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI

DSGA e Ass. Amministrativi

Al fine di agevolare i lavori inerenti all'applicazione della normativa relativa al trattamento dei dati personali, ai sensi degli artt. 33, 34, 35 del D. Lgs. 30 giugno 2003 n. 196, si impartiscono le istruzioni alle quali il funzionario incaricato del trattamento dei dati del personale della scuola e delle ditte e/o collaboratori esterni, siano essi soggetti singoli o enti e associazioni, deve attenersi:

Art. 34 (Trattamenti con strumenti elettronici)

1. Il trattamento di dati personali con strumenti elettronici è consentito mediante credenziali di autenticazione, cioè mediante un codice per l'identificazione associato a una parola chiave riservata conosciuta solamente dalla S.V.

2. La S.V. è tenuta ad adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso Suo esclusivo. In particolare, oltre alla custodia personale delle credenziali assegnate, copia di esse deve essere depositata al custode delle password. 3. Ogni 3 mesi modificherà codice e parola chiave delle credenziali garantendo i livelli di segretezza dovuti, con la collaborazione dell'Amministratore di sistema.

4. Durante la sessione di trattamento, lo strumento elettronico **non deve essere accessibile** ad altri soggetti estranei all'incarico assegnatoLe

5. Al termine della giornata lavorativa del sabato, la S.V. provvederà a effettuare il salvataggio dei dati.

Art. 35 (Trattamenti senza l'ausilio di strumenti elettronici)

1 - La S.V. è tenuta al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati del personale della scuola e dei collaboratori esterni situati negli appositi e riservati arredi d'ufficio. A tal fine l'accesso agli archivi e/o agli armadi metallici di sicurezza non deve essere consentito ad altri soggetti estranei all'incarico assegnatoLe.

2 - Durante il trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dalla S.V. fino alla ricollocazione in archivio e/o in armadio in maniera che ad essi non accedano persone prive di autorizzazione.

3 - Non è ammesso l'accesso all'archivio a persone, a qualunque titolo, dopo l'orario di chiusura dell'ufficio.

Gli ambiti di trattamento dei dati personali e sensibili degli operatori della scuola e dei collaboratori/ditte esterni sono così individuati:

- assunzione e cessazione dal servizio;
- aggiornamento dei dati personali;
- acquisizione e rilascio di certificazioni, attestati, diagnosi, denunce, atti interni e esterni;
- concessione di contributi, finanziamenti, elargizioni ed altri benefici previsti dalla legge, dai regolamenti o dalla normativa comunitaria, anche in favore di associazioni, fondazioni ed enti;
- riconoscimento di esoneri, agevolazioni o riduzioni tariffarie o economiche, franchigie, o al rilascio di concessioni;
- sanzioni amministrative e ricorsi;
- riconoscimento della causa di servizio o dell'equo indennizzo, nonché ad obblighi retributivi, fiscali o contabili, relativamente al personale in servizio o in quiescenza, ivi compresa la corresponsione di premi e benefici assistenziali;

- anagrafe dei pubblici dipendenti e applicazione della normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti;

- applicazione della normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale

- comunicazioni generiche

- comunicazioni con enti e istituzioni

Per una coerente applicazione della legge, si riporta quanto disposto dall'art. 20 (Principi applicabili al trattamento di dati sensibili) del D.Lgs. 196/2003:

"1. *Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se 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.*

2. 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, il trattamento è consentito 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."

Per opportuna conoscenza, si richiama la definizione che l'art. 4 del D. Lgs 196/2003 dà al termine di **"dato sensibile":** *i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.*

Alla luce della definizione di cui sopra, sono da intendersi "dati sensibili":

- i certificati medici, riportanti la patologia, relativi allo stato di salute del personale;

- i dati relativi ai soggetti portatori di handicap;

- dati relative a situazioni particolari familiari (separazioni; trattamenti cautelari, etc.)

- provvedimenti amministrativi di carattere disciplinare;

Per ciò che attiene tali ambiti, il trattamento dei dati deve prevedere forme inintelliggibili di scrittura e di comunicazione.

I dati sensibili saranno conservati, negli appositi armadi metallici di sicurezza, in buste chiuse e controfirmate dagli incaricati del trattamento e saranno aperti su richiesta motivata a cura del titolare o dei responsabili del trattamento dei dati personali.

DICHIARAZIONE DI IMPEGNO

Il Dirigente Scolastico - titolare del trattamento dei dati - si impegna ad adottare, con la consulenza del **responsabile del trattamento e del Responsabile della protezione dei dati ai sensi del regolamento UE/2016**, nella fase di graduale attuazione degli interventi previsti dalla normativa sulla tutela della privacy, ogni possibile misura destinata a salvaguardare la sicurezza dei dati personali, siano essi contenuti nei documenti cartacei che registrati mediante strumenti elettronici. Tali misure riguarderanno gli aspetti organizzativi, logistici e procedurali miranti ad evitare con ogni mezzo qualsiasi incremento di rischi di distruzione o perdita, anche accidentale, dei dati oggetto di trattamento, di accesso non autorizzato o di trattamento non consentito nel rispetto delle misure minime ICT previste dall'Istituzione scolastica ai sensi della **Direttiva PCM del 01/08/2015 e della CIRCOLARE 18 aprile 2017, n. 2/2017**

Responsabile della protezione dei dati
(Ins. Gerlando Alonge)

Il Titolare
Dirigente Scolastico
(Dott.Silvana Spirio)

Il Dirigente Scolastico
(Dott. SILVANA SPIRIO)