I.P.S.I.A. "Majorana"

Via Volta, 11 20063 Cernusco Sul Naviglio (MI)

DOCUMENTO delle MISURE a TUTELA dei DATI delle PERSONE

Redatto ai sensi e per gli effetti degli artt. 24 comma 1, 30 e 35 del Regolamento dell'Unione Europea 2016/679

Contiene:

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO (Art. 30 Reg. UE)
VALUTAZIONE D'IMPATTO (D.P.I.A.) (Art. 35 Reg. UE)

Relativa ai seguenti trattamenti

AMMINISTRAZIONE DEGLI STUDENTI
TRATTAMENTO GIURIDICO ED ECONOMICO DEL PERSONALE

Data di elaborazione del documento : **09/12/2019**

DOCUMENTO CON VALIDITA' ANNUALE

REV. 5.0

STUDIO TECNICO LEGALE
CORBELLINI
Studio AG.I.COM. S.r.l.

Redatto a cura del D.P.O. negli uffici di :

STUDIO AG.I.COM. S.R.L. UNIPERSONALE
Via XXV Aprile, 12 - SAN ZENONE AL LAMBRO (MI)
Tel. 02 90601324 Fax 02 700527180
E-mail info@agicomstudio.it

SEDI IN CUI VENGONO TRATTATI I DATI (LUOGHI)

Al Responsabile della protezione dei dati è affidato il compito di redigere e di aggiornare, ad ogni variazione, l'elenco delle sedi in cui viene effettuato il trattamento dei dati delle persone.
Indipendentemente dal luogo ove viene eseguito il trattamento, il Responsabile della protezione dei dati vigila affinchè esso avvenga entro locali sicuri e ad opera di personale autorizzato.

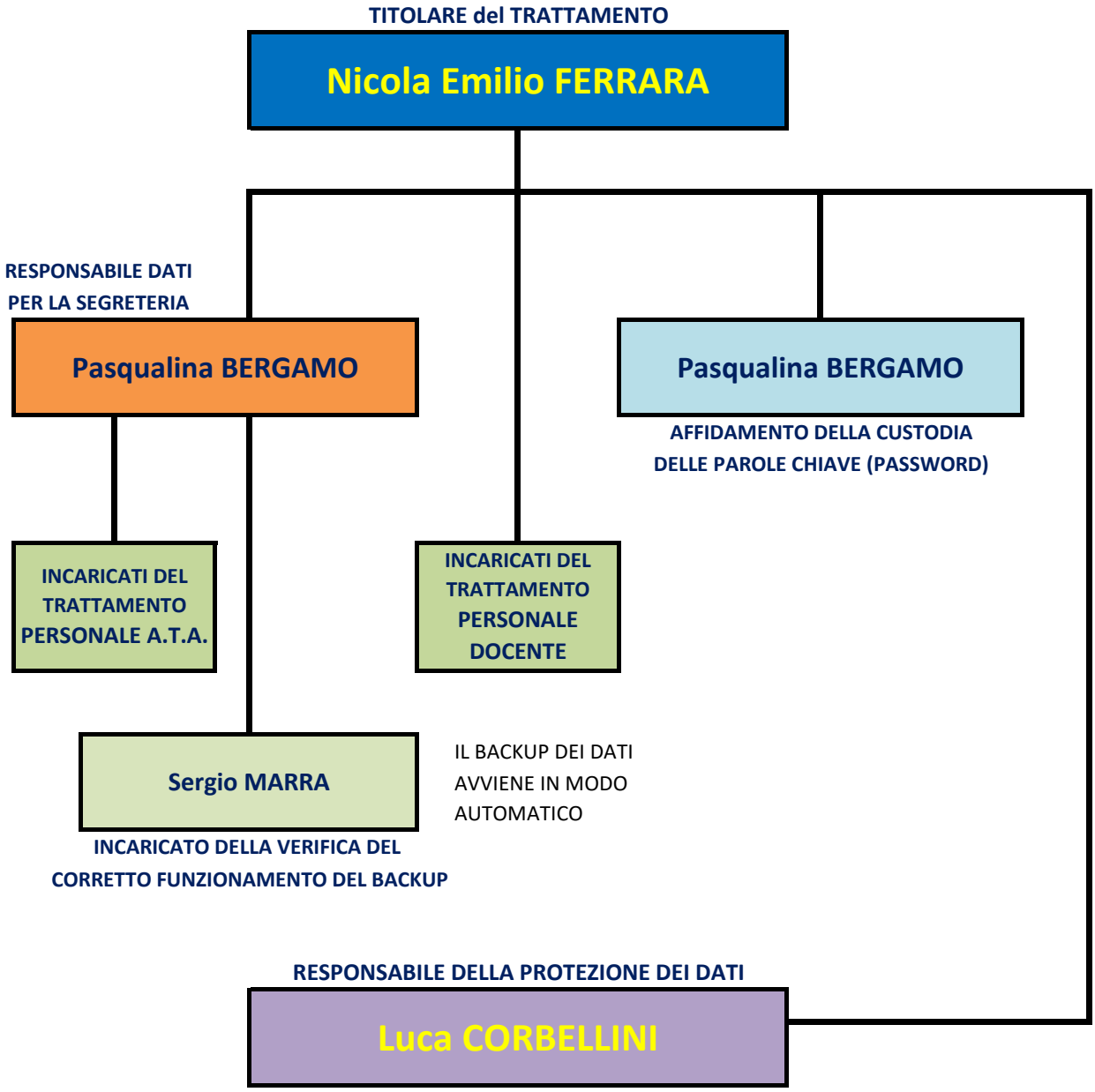
Per l'ente in oggetto le sedi in cui avviene il trattamento sono:

Tabella A

SEDE LEGALE

I.P.S.I.A. "Majorana"	Via Volta, 11, 20063 - Cernusco Sul Naviglio (MI)

ORGANIGRAMMA DELLA PRIVACY (PERSONE)



Il trattamento dei dati personali deve avvenire esclusivamente a cura di taluni soggetti ben individuati dalla legge (Titolare del trattamento), dal Titolare del trattamento (Responsabili del trattamento e Custodi delle password) o dal Responsabile del trattamento (Incaricati del trattamento).
A nessuno, al di fuori di questa sfera di soggetti, è consentito di venire in contatto con i dati personali.

In questa pagina del documento vengono individuati nominalmente, alla data di redazione dello stesso, i soggetti su cui è imperniato il trattamento dei dati all'interno dell'Istituto.

Di seguito invece indicheremo le classi (gruppi) di incaricati presenti all'interno della struttura e definiremo i poteri assegnati a ciascuno. La definizione nominativa sempre aggiornata degli Incaricati del trattamento, attesa la frequente precarietà dell'incarico, è lasciata alle lettere di incarico.

ORGANIGRAMMA DELLA PRIVACY (INCARICATI DEL TRATTAMENTO)

X	TITOLARE
S	SUPPLENTE

RIFERIMENTO PROFILI DI AUTORIZZAZIONE DEGLI INCARICATI DEL TRATTAMENTO (D.M.T.D.P.)

NOME e COGNOME	FUNZIONE	STUDENTI	DIPENDENTI	FORNITORI		PROTOCOLLO	POSTA ELETTRONICA
Antonella PETTINE	ASSISTENTE AMMINISTRATIVO	X	S			X	X
Rosita LENZA	ASSISTENTE AMMINISTRATIVO	S	X			X	X
Maria Lucrezia PITTELLA	ASSISTENTE AMMINISTRATIVO		X	X		X	X
Marinella PIAZZA	ASSISTENTE AMMINISTRATIVO	X	S			X	X
Francesca TOMAINO	ASSISTENTE AMMINISTRATIVO		X			X	X

NOME e COGNOME	FUNZIONE	ARCHIVIO (*)
Giuseppe CAPOLUPO	COLLABORATORE DEL DIRIGENTE SCOLASTICO	ALLIEVI
Maria Rosa PELIZZOLI	COLLABORATORE DEL DIRIGENTE SCOLASTICO	ALLIEVI
Gaetano OTTAVIANO	REFERENTE ALTERNANZA	ALLIEVI
Roberto LIMONTA	REFERENTE ALTERNANZA	ALLIEVI
Vincenzo TARANTINO	R.L.S. (SICUREZZA)	ALL. & PERS.
Vincenzo TARANTINO	FUNZIONE STRUMENTALE: BES	ALLIEVI
Francesco MARINCOLA	SITO	ALL. & PERS.
Pietro PIERRO	A.S.P.P. (SICUREZZA)	ALL. & PERS.

(*) Archivio dati a cui l'incaricato ha accesso.

INDICE

I. SCOPO DEL DOCUMENTO

Scopo di questo documento è di delineare il quadro delle misure minime di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato all'interno della struttura, al fine di conoscere il proprio stato di sicurezza rispetto ai rischi di violazione della riservatezza e perdita di dati.
Esso viene redatto ogni anno per garantire una perfetta aderenza del contenuto dello stesso alle modificate esigenze di sicurezza nonché, al variare nel tempo, del profilo dei rischi incombenti sui dati.

Il modello grafico adottato è stato realizzato in proprio dallo Studio AG.I.COM. S.r.l. sulla base della specifica esperienza acquisita fin dal 1996 in seguito all'entrata in vigore della Legge n° 675 che può definirsi come la prima vera e propria normativa sulla privacy che l'Italia si è data.

All'interno del documento vengono definiti i criteri per:

I. La protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
II. I criteri e le procedure per assicurare l'integrità dei dati;
III. I criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per via telematica;
IV. L'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

Il presente documento è redatto e firmato in calce dal Titolare del trattamento e dal Responsabile della Protezione dei Dati (R.P.D. – D.P.O.).

II. AMBITO DI APPLICAZIONE DEL DOCUMENTO

Il presente documento è applicato ai trattamenti di dati che avvengono all'interno delle strutture di competenza del titolare, ovunque esse si trovino sul territorio italiano.

Si forniscono inoltre idonee informazioni riguardanti:

a) l'elenco dei trattamenti di dati personali mediante :

- Individuazione tipologia di dati trattati
- Descrizione aree, locali e strumenti con cui si esegue il trattamento
- Elaborazione mappa dei trattamenti effettuati

b) la distribuzione dei compiti e delle responsabilità e la previsione di interventi formativi degli incaricati individuati dal presente;

c) l'analisi dei rischi che incombono sui dati;

d) le misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati;

e) i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento;

f) i criteri da adottare per garantire l'adozione delle misure minime di sicurezza dei dati

g) le procedure per seguire il controllo dello stato di sicurezza

Le procedure contenute nel presente documento devono essere conosciute ed applicate da tutti gli uffici ed i reparti su cui è strutturato l'ente titolare del trattamento.

III. FONTI DEL DIRITTO

Il Documento delle Misure a Tutela dei Dati delle Persone e le disposizioni che esso contiene sono conformi a quanto previsto dagli articoli 24 comma 1, 30 e 35 del Regolamento dell'Unione Europea 2016/679.

Con particolare riferimento alla tipologia del soggetto obbligato alla redazione del presente documento, Istituto di Istruzione Statale, esso è conforme ai principi indicati nel Decreto del Ministro della Pubblica Istruzione N° 305 del 15 Gennaio 2007, denominato anche "Regolamento per i dati sensibili e giudiziari del Ministero della Pubblica Istruzione".

IV. SOGGETTI DEL TRATTAMENTO DEI DATI

La normativa vigente ha definito talune figure fondamentali a cui attribuisce ruoli chiave nei vari passaggi su cui è strutturato il trattamento dei dati.

Queste figure sono:

IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

La persona giuridica o l'Istituzione statale è, "*ope legis*", per mezzo del suo rappresentante legale, TITOLARE DEL TRATTAMENTO.
Quale Titolare del trattamento gli è consentito individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati, che assicurino che vengano adottate le misure di sicurezza minime previste dalla legge per il trattamento dei dati come le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite per iscritto dal Titolare stesso

IL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

In relazione all'attività del Titolare del trattamento, è prevista come facoltativa, la nomina del Responsabile del trattamento, con compiti specifici in relazione alle funzioni svolte. Il Titolare del trattamento se vuole, affida al Responsabile del trattamento l'onere di individuare, nominare ed indicare per iscritto uno o più Incaricati del trattamento appartenenti alla propria organizzazione.

Il Titolare (ed il Responsabile del trattamento dei dati se designato) hanno il compito di:

- Redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete pubblica, nonché l'elenco dei trattamenti effettuati;
- Attribuire ad ogni Utente (USER) o incaricato un Codice identificativo personale (USER ID) per l'utilizzazione dell'elaboratore, che deve essere individuale e non riutilizzabile;
- Autorizzare i singoli incaricati del trattamento e della manutenzione, qualora utilizzino elaboratori accessibili in rete e nel caso di trattamento di dati sensibili e giudiziari; per gli stessi dati, qualora il trattamento sia effettuato tramite elaboratori accessibili in rete disponibile al pubblico, saranno oggetto di autorizzazione anche gli strumenti da utilizzare;
- Verificare, con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire le modalità di accesso ai locali;
- Garantire che tutte le misure di sicurezza riguardanti i dati in possesso della società siano applicate all'interno ed eventualmente al di fuori della stessa, qualora cedute a soggetti terzi, quali Responsabili del trattamento, tutte o parte delle attività di trattamento;

Il Titolare del trattamento dei dati deve informare il Responsabile del trattamento dei dati delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, e dall'accordo contrattuale o di altra natura che egli ha concluso con questo.

La nomina del Responsabile del trattamento può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

INCARICATI DEL TRATTAMENTO DEI DATI

Al Titolare del trattamento (ed al Responsabile del trattamento se nominato e per quanto attiene alla propria struttura) è affidato il compito di nominare, con comunicazione scritta, uno o più Incaricati del trattamento dei dati. La nomina di ciascun Incaricato del trattamento dei dati deve essere effettuata con lettera di incarico in cui sono specificati i compiti che gli sono affidati.
Gli Incaricati del trattamento devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.
Agli incaricati deve essere assegnata una parola chiave e un codice identificativo personale.
La nomina degli incaricati del trattamento deve essere controfirmata dall'interessato per presa visione e copia della stessa deve essere conservata a cura del Responsabile del trattamento per la sicurezza dei dati in luogo sicuro.
Agli Incaricati del trattamento il Responsabile del trattamento per la sicurezza dei dati deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina degli incaricati è a tempo indeterminato e decade per revoca, per dimissioni o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

CUSTODE DELLE PAROLE CHIAVE

È compito del Custode delle parole chiave gestire e custodire le *password* per l'accesso ai dati da parte degli incaricati.
Il Custode delle parole chiave deve predisporre, per ogni Incaricato del trattamento, una busta sulla quale è indicato lo USER ID utilizzato: all'interno della busta deve essere indicata la *password* usata per accedere alla banca di dati.
Le buste con le *password* debbono essere conservate in luogo sicuro e protetto.
Il Custode delle parole chiave deve revocare tutte le *password* non utilizzate per un periodo superiore a sei (6) mesi.
Il Titolare del trattamento nomina un Custode delle parole chiave a cui è conferito il compito di custodire le *password* per l'accesso ai dati archiviati nei sistemi di elaborazione dei dati.
La nomina del Custode delle parole chiave deve essere effettuata con lettera di incarico.
La nomina di Custode delle parole chiave deve essere controfirmata dall'interessato per presa visione e copia della nomina accettata deve essere conservata in luogo sicuro a cura del Responsabile del trattamento, se diverso dal Custode delle parole chiave.
Il Responsabile del trattamento deve informare il Custode delle parole chiave della responsabilità che gli è stata affidata in relazione a quanto disposto dalle normative in vigore

La nomina del Custode delle parole chiave è a tempo indeterminato e decade per revoca o per dimissioni dello stesso.

La nomina del Custode delle parole chiave può essere revocata in qualsiasi momento dal Titolare del trattamento senza preavviso ed essere affidata ad altro soggetto.

V. INDIVIDUAZIONE DEI TRATTAMENTI DEI DATI EFFETTUATI

Al Titolare del trattamento (ed al Responsabile del trattamento dei dati se designato e per quanto di sua competenza) è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati (Registro delle attività di trattamento).

Ogni banca di dati o archivio cartaceo deve essere classificato in relazione alle informazioni in esso contenute indicando se si tratta di dati personali, sensibili, giudiziari o altro.

A fini classificatori abbiamo ritenuto utile suddividere i trattamenti di competenza del Titolare scrivente secondo questa logica:

Tabella B	Trattamenti dati eseguiti all'interno dei luoghi di cui alla Tabella A
Tabella B1	Trattamento dei dati degli allievi (Amministrazione degli studenti)
Tabella B2	Trattamento economico e giuridico del personale
Tabella B3	Trattamento dei dati dei fornitori e degli specialisti esterni
Tabella B4	Trattamento non ordinario
Tabella B5	Trattamento non ordinario
Tabella C	Trattamenti dati affidati a soggetti esterni alla struttura del Titolare
Tabella D	Trattamenti eseguiti da ciascuna categoria ammessa al trattamento dei dati personali

Tabella B

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

ID	Descrizione sintetica del Trattamento
T1	**Assistenza scolastica (amministrazione degli studenti)** ISCRIZIONE PRATICHE ALLIEVI D.V.A. DENUNCE INFORTUNI ALLIEVI ESAMI DI STATO TENUTA REGISTRO DIPLOMI CERTIFICAZIONI ALLIEVI RICH. / TRASM. DOCUMENTI ALLIEVI NULLAOSTA CORRISPONDENZA SCUOLA-GENITORI VERBALI ORGANI COLLEGIALI OSSERVATORIO OBBLIGO FORMATIVO SPORTELLO DIDATTICA
T2	**Trattamento giuridico ed economico del personale dipendente** GESTIONE DELLE GRADUATORIE RACCOLTA INIZIALE DATI DIPENDENTI STIPULA CONTRATTI DI LAVORO RILEVAZIONE ASSENZE PERSONALE ELABORAZIONE RETRIBUZIONI RICOSTRUZIONE CARRIERA ISTRUZIONE PRATICHE DI PENSIONE DENUNCE INFORTUNI PERSONALE GESTIONE DOMANDE PRESTITI PERSONALI PRATICHE PROCEDIMENTI DISCIPLINARI CERTIFICAZIONI PERSONALE PRATICHE MOBILITA' PERSONALE PRATICHE INIDONEITA' PERSONALE PRATICHE EX LEGGE 104 770 / IRAP PERMESSI SINDACALI GESTIONE T.F.R. PERMESSI – CONGEDI – FERIE RICH./ TRASM. DOCUMENTI PERSONALE RISCATTO PENSIONE E LIQUIDAZIONE SCIOPERO – TRASMISSIONE DATI
T3	**Gestione fornitori di beni e servizi**
T4	**Gestione posta elettronica e cartacea**

Tabella B1

DESCRIZIONE DEI TRATTAMENTI DI DATI PERSONALI ESEGUITI

				TRATTAMENTI CARTACEI		TRATTAMENTI ELETTRONICI		
ID	Denominazione banca dati	Categorie interessate	Natura dei dati (1)	Strutture entro le quali avviene il trattamento cartaceo	Strutture di archiviazione storica dei dati cartacei trattati	Struttura entro la quale avviene il trattamento informatico	Struttura di archiviazione informatica e back-up dei dati	Moduli segreteria digitale
T1a	**Assistenza scolastica (amministrazione degli studenti)** ISCRIZIONE ALLIEVI PRATICHE ALLIEVI D.V.A. DENUNCE INFORTUNI ALLIEVI ESAMI DI STATO TENUTA REGISTRO DIPLOMI CERTIFICAZIONI ALLIEVI RICH. / TRASM. DOCUMENTI ALLIEVI NULLAOSTA CORRISPONDENZA SCUOLA-GENITORI VERBALI ORGANI COLLEGIALI OSSERVATORIO OBBLIGO FORMATIVO SPORTELLO DIDATTICA	ALLIEVI GENITORI TUTORI	P/S/G	Segreteria didattica Presidenza Vicepresidenza Sala docenti	Archivio didattico	CLOUD	CLOUD	PROTOCOLLO PROT. RISERV. ALUNNI BIBLIOTECA
T1d	**Assistenza scolastica (amministrazione degli studenti)** GESTIONE DEL REGISTRO ELETTRONICO		P/S/G	NON PERTINENTE	NON PERTINENTE	CLOUD	CLOUD	Metodo di consultazione in uso: PERSONAL COMPUTER

TERMINE ENTRO IL QUALE I DATI VENGONO DISTRUTTI	
FASCICOLI PERSONALI	ILLIMITATA
ACCERTAMENTI SANITARI RIFERITI AD INFORTUNI	ILLIMITATA
REGISTRI DI ISCRIZIONE / IMMATRICOLAZIONE DEGLI ALLIEVI	ILLIMITATA
REGISTRI GENERALI DEI VOTI E DELLE VALUTAZIONI E PAGELLA DI SCRUTINIO	50 ANNI
DATI RELATIVI A BORSE DI STUDIO	50 ANNI
ELABORATI PROVE SCRITTE PER GLI ESAMI DI STATO	ILLIMITATA
ELENCHI BUONI LIBRO E CEDOLE LIBRARIE [CONSERVARE 1 ESEMPLARE A CAMPIONE]	6 ANNI
ELENCHI SERVIZIO MENSA [CONSERVARE 1 ESEMPLARE A CAMPIONE]	6 ANNI
REGISTRI DELLE ASSENZE DEGLI ALLIEVI [CONSERVARE 1 ESEMPLARE A CAMPIONE]	6 ANNI
PROVE SCRITTE (ECCETTO ESAMI DI STATO) [CONSERVARE INTERA ANNATA OGNI 10]	1 ANNO

PROCEDURE DI SICUREZZA ATTIVE
Sono attivi profili di autorizzazione diversi per ogni incaricato
L'accesso ai dati avviene mediante chiave fisica o password
E' applicata una procedura di cambio password periodico (3 o 6 mesi)
Le password in uso sono considerate "complesse"
E' prevista la distruzione dei supporti informatici non più in uso
E' prevista la distruzione dei documenti cartacei da eliminare
Le procedure vengono riesaminate con cadenza annuale come i profili
Viene eseguita dai server la registrazione ed il controllo degli accessi
Sono attivi programmi di formazione dei soggetti incaricati del trattam.
E' implementato un sistema di back-up + disaster recovery dei dati
I locali sono dotati di sistemi anti-intrusione
I locali sono dotati di presidi antincendio
L'Impianto elettrico è dotato di misure atte ad evitare sovraccarichi

(1) P = Meramente personali S = Particolari (Sensibili) G = Giudiziari

Tabella B2

DESCRIZIONE DEI TRATTAMENTI DI DATI PERSONALI ESEGUITI

				TRATTAMENTI CARTACEI		TRATTAMENTI ELETTRONICI		
ID	Denominazione banca dati	Categorie interessate	Natura dei dati (1)	Strutture entro le quali avviene il trattamento cartaceo	Strutture di archiviazione storica dei dati cartacei trattati	Struttura entro la quale avviene il trattamento informatico	Struttura di archiviazione informatica e back-up dei dati	Moduli segreteria digitale
T2	**Trattamento giuridico ed economico del personale** GESTIONE DELLE GRADUATORIE RACCOLTA INIZIALE DATI DIPENDENTI STIPULA CONTRATTI DI LAVORO RILEVAZIONE ASSENZE PERSONALE ELABORAZIONE RETRIBUZIONI RICOSTRUZIONE CARRIERA ISTRUZIONE PRATICHE DI PENSIONE DENUNCE INFORTUNI PERSONALE GESTIONE DOMANDE PRESTITI PERS. PRATICHE PROCEDIMENTI DISCIPLINARI PRATICHE MOBILITA' PERSONALE PRATICHE INIDONEITA' PERSONALE PRATICHE EX LEGGE 104 770 / IRAP PERMESSI SINDACALI GESTIONE T.F.R. PERMESSI – CONGEDI – FERIE RICH./ TRASM. DOCUMENTI PERSONALE	Personale Docente e non Docente	P/S/G	Segreteria personale Presidenza Vicepresidenza	Archivio del personale	CLOUD	CLOUD	PROTOCOLLO PROT. RISERV. PERSONALE RIL. PRESENZE Metodo di consultazione in uso: PERSONAL COMPUTER	

TERMINE ENTRO IL QUALE I DATI VENGONO DISTRUTTI	
REGISTRI DEI CONTRATTI	ILLIMITATA
DATI RELATIVI A PROCEDIMENTI DISCIPLINARI E GIUDIZIARI	ILLIMITATA
CONTRATTI DI ASSUNZIONE E PRESTAZIONE D'OPERA	ILLIMITATA
FASCICOLI PERSONALI	ILLIMITATA
ACCERTAMENTI SANITARI RELATIVI A MALATTIE PROFESSIONALI E INFORTUNI	ILLIMITATA
ORARIO DI SERVIZIO E REGISTRO DELLE ASSENZE	50 ANNI
REISTRI DEGLI STIPENDI E DEGLI ALTRI ASSEGNI	50 ANNI
DOMANDE DI FERIE E PERMESSI [CONSERVARE 1 ESEMPLARE A CAMPIONE]	6 ANNI
COPIE CERTIFICATI DI SERVIZIO [CONSERVARE 1 ESEMPLARE A CAMPIONE]	6 ANNI
RICHIESTE DI ACCESSO A COPIE DI ATTI	1 ANNO

PROCEDURE DI SICUREZZA ATTIVE
Sono attivi profili di autorizzazione diversi per ogni incaricato
L'accesso ai dati avviene mediante chiave fisica o password
E' applicata una procedura di cambio password periodico (3 o 6 mesi)
Le password in uso sono considerate "complesse"
E' prevista la distruzione dei supporti informatici non più in uso
E' prevista la distruzione dei documenti cartacei da eliminare
Le procedure vengono riesaminate con cadenza annuale come i profili
Viene eseguita dai server la registrazione ed il controllo degli accessi
Sono attivi programmi di formazione dei soggetti incaricati del trattam.
E' implementato un sistema di back-up + disaster recovery dei dati
I locali sono dotati di sistemi anti-intrusione
I locali sono dotati di presidi antincendio
L'Impianto elettrico è dotato di misure atte ad evitare sovraccarichi

(1) P = Meramente personali S = Particolari (Sensibili) G = Giudiziari

Tabella B3

Tabella B3

DESCRIZIONE DEI TRATTAMENTI DI DATI PERSONALI ESEGUITI

				TRATTAMENTI CARTACEI		TRATTAMENTI ELETTRONICI		
ID	Denominazione banca dati	Categorie interessate	Natura dei dati (1)	Strutture entro le quali avviene il trattamento cartaceo	Strutture di archiviazione storica dei dati cartacei trattati	Struttura entro la quale avviene il trattamento informatico	Struttura di archiviazione informatica e back-up dei dati	Moduli segreteria digitale
T3	**Gestione fornitori di beni e servizi e degli specialisti esterni**	Fornitori e Specialisti	P/G	Segreteria contabile Ufficio D.S.G.A. Presidenza Vicepresidenza	Archivio contabile e amministrativo	CLOUD	CLOUD	PROTOCOLLO BILANCIO UFF. TECNICO MAGAZZINO Metodo di consultazione in uso: PERSONAL COMPUTER

TERMINE ENTRO IL QUALE I DATI VENGONO DISTRUTTI	
ORDINI	10 ANNI
FATTURE	10 ANNI
CASELLARI GIUDIZIARI	10 ANNI
I DOCUMENTI CONTABILI RIMANGONO AGLI ATTI PERMANENTEMENTE	

PROCEDURE DI SICUREZZA ATTIVE
Sono attivi profili di autorizzazione diversi per ogni incaricato
L'accesso ai dati avviene mediante chiave fisica o password
E' applicata una procedura di cambio password periodico (3 o 6 mesi)
Le password in uso sono considerate "complesse"
E' prevista la distruzione dei supporti informatici non più in uso
E' prevista la distruzione dei documenti cartacei da eliminare
Le procedure vengono riesaminate con cadenza annuale come i profili
Viene eseguita dai server la registrazione ed il controllo degli accessi
Sono attivi programmi di formazione dei soggetti incaricati del trattam.
E' implementato un sistema di back-up + disaster recovery dei dati
I locali sono dotati di sistemi anti-intrusione
I locali sono dotati di presidi antincendio
L'Impianto elettrico è dotato di misure atte ad evitare sovraccarichi

(1) P = Meramente personali S = Particolari (Sensibili) G = Giudiziari

Le credenziali amministrative dei server citati alle Tabelle Bx sono nella disponibilità di:

Tipologia di accesso	Ruolo	Server	Nome e Cognome
Administrator	AMM. DI RETE	SEGRETERIA	Sergio MARRA
	D.S.G.A.	SEGRETERIA	Vincenzo BONASSO
	TECNICO AXIOS	SEGRETERIA	Luciano SASSO
	TECNICO PC	SEGRETERIA	Sergio MANGOGNA

I soggetti incaricati della gestione a livello amministrativo dei Server ove avviene il trattamento dei dati delle persone, ivi compresi quelli particolari (sensibili) e giudiziari eventualmente presenti, nonché degli apparati attivi di rete (switch, firewall etc.) al fine di attuare le misure minime di sicurezza informatiche sono:

Rete di riferimento	Nome e Cognome	Dipendente o Esterno
ASSISTENZA TECNICA SUL SERVER DI SEGRETERIA E SEGRETERIA DIGITALE		
ASSISTENZA TECNICA SUL REGISTRO ELETTRONICO E SOFTWARE DIDATTICI		

Visto quanto previsto al punto 2.c del Provvedimento del Garante per la protezione dei dati personali del 27 Novembre 2008 recante :"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato sulla Gazzetta Ufficiale n. 300 del 24 Dicembre 2008, gli estremi identificativi dell'Amministratore di sistema di questo Istituto sono di seguito resi noti secondo quanto stabilito al comma 4.3 :

Rete di riferimento	Nome e Cognome	Dipendente o Esterno
Incaricato di sovraintendere alla gestione ed amministrazione del sistema informatico in generale.	Sergio MARRA	DIPENDENTE

Il curriculum vitae dell'incaricato è allegato, a cura del titolare, al seguente documento

Alcuni trattamenti di dati personali possono essere affidati all'esterno della struttura del Titolare, per questi è mandatorio indicarne gli estremi, identificare il soggetto esterno e formalizzare con questi un contratto di trattamento dal quale si evinca la sussistenza di un obbligo giuridico di adempimento degli impegni assunti da questo in ordine alla applicazione del Regolamento U.E. ed alla regolare tenuta dei dati a lui affidati :

Tabella C

CENSIMENTO DEI TRATTAMENTI DATI AFFIDATI ALL'ESTERNO

ID	Descrizione sintetica dell'attività esternalizzata	Trattamenti interessati	Soggetto esterno	Descrizione criteri ed impegni assunti dal soggetto esterno per l'adozione delle misure minime di sicurezza dei dati
E1	**Adempimenti e formazione in materia di SICUREZZA DEI DATI PERSONALI (PRIVACY) (Regolamento UE 2016/679)**	T1a T2	Studio AG.I.COM. S.r.l. Via XXV Aprile, 12 SAN ZENONE AL LAMBRO (MI)	Il soggetto esterno assume l'incarico di RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI e si obbliga ai doveri di riservatezza e di organizzazione previsti dal G.D.P.R. per chi esercita un trattamento in proprio o conto terzi
E2	**Adempimenti e formazione in materia di SICUREZZA ed IGIENE DEL LAVORO (D.Lgs 81/2008)**	T1a T2	DA DEFINIRE	Il soggetto esterno assume l'incarico di RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI e si obbliga ai doveri di riservatezza e di organizzazione previsti dal G.D.P.R. per chi esercita un trattamento in proprio o conto terzi
E3	**Attività di sorveglianza sanitaria MEDICO COMPETENTE**	T2	Dott. Marco TASCA MEDLAV S.R.L. Viale Giulio Cesare, 3 24124 - Bergamo (BG)	Il soggetto esterno assume l'incarico di RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI e si obbliga ai doveri di riservatezza e di organizzazione previsti dal G.D.P.R. per chi esercita un trattamento in proprio o conto terzi
E4	**Servizio di SUPPORTO PSICOLOGICO a Studenti, Genitori e Docenti dell'Istituto**	T1d T2	Dott.ssa Nicoletta SASSO Via Volta, 11 20063 - Cernusco Sul Naviglio (MI)	Il soggetto esterno assume l'incarico di RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI e si obbliga ai doveri di riservatezza e di organizzazione previsti dal G.D.P.R. per chi esercita un trattamento in proprio o conto terzi
E5				
E6				
E7				
E8				
E9				

In considerazione della difficoltà di eseguire controlli e verifiche presso strutture esterne alla propria, il Titolare del Trattamento, acquisito il parere concorde del Responsabile della Protezione dei Dati, ritiene di dover richiedere al soggetto esterno, a garanzia della corretta esecuzione degli obblighi derivanti dal trattamento affidato, una autocertificazione circa l'osservanza delle Misure Minime di Sicurezza previste dalle norme vigenti.

Resta comunque salvo l'obbligo, per tutti gli incaricati del trattamento che intrattengono rapporti con il soggetto esterno, di richiamare l'osservanza delle misure minime nonché di segnalare, senza ritardo alcuno, al Responsabile della Protezione dei dati, eventuali difformità rispetto a quanto autocertificato.

VI. INDIVIDUAZIONE DEI TRATTAMENTI ESEGUITI PER CATEGORIA

All'interno del comparto scolastico è facile associare taluni trattamenti dati ad alcune categorie di lavoratori operanti all'interno della struttura del titolare. Ferme restando le peculiarità emergenti dalle lettere di incarico consegnate ai singoli incaricati del trattamento, rileviamo alcuni tratti comuni:

TRATTAMENTI ESEGUITI DA CIASCUNA CATEGORIA AMMESSA AL TRATTAMENTO DI DATI PERSONALI

Tabella D

ID	Denominazione categoria	Banche dati a cui ha accesso	Struttura di riferimento	Strumenti CARTACEI	Strumenti INFORMATICI
DS	DIRIGENTE SCOLASTICO	1) FASCICOLI DI TUTTO IL PERSONALE 2) VERBALI ASSEMBLEE ORGANI COLLEGIALI 3) PROGRAMMAZ. RELATIVA STATO DI DISAGIO DI ALLIEVI 4) PROTOCOLLO RISERVATO 5) FASCICOLO DEL PERSONALE IN PROVA 6) REGISTRI DI CLASSE E PERSONALI DEL DOCENTE	Dirigenza	Armadio e cassettiera	Archivio software gestionale Gestione anagrafica Allievi Gestione Esiti finali Gestione anagrafica Personale Gestione Trasferimenti Gestione Rapporti EE.LL. Gestione Rapporti ASL Gestione graduatorie Gestione Infortuni Gestione Posta elettronica Archivio Microsoft OFFICE
DA	DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI	1) FASCICOLI DI TUTTO IL PERSONALE 2) ANAGRAFE DEI FORNITORI ED I CONTRATTI 3) DOCUMENTAZIONE CONTABILE E FINANZIARIA 4) DOCUMENTAZIONE DIDATTICA DA ARCHIVIARE 5) REGISTRO INFORTUNI 6) PROTOCOLLO	Ufficio D.S.G.A. Segreteria Archivio	Armadio e cassettiera	Archivio software gestionale Gestione anagrafica Allievi Gestione Esiti finali Gestione anagrafica Personale Gestione Trasferimenti Gestione Rapporti EE.LL. Gestione Rapporti ASL Gestione graduatorie Gestione Infortuni Gestione Posta elettronica Archivio Microsoft OFFICE
AA	ASSISTENTE AMMINISTRATIVO	1) FASCICOLI DI TUTTO IL PERSONALE 2) ANAGRAFE DEI FORNITORI ED I CONTRATTI 3) DOCUMENTAZIONE CONTABILE E FINANZIARIA 4) DOCUMENTAZIONE DIDATTICA DA ARCHIVIARE 5) REGISTRO INFORTUNI 6) PROTOCOLLO	Segreteria Archivio	Armadi e cassettiera	Archivio software gestionale Gestione anagrafica Allievi Gestione Esiti finali Gestione anagrafica Personale Gestione Trasferimenti Gestione Rapporti EE.LL. Gestione Rapporti ASL Gestione graduatorie Gestione Infortuni Gestione Posta elettronica Archivio Microsoft OFFICE
D	DOCENTE	1) REGISTRO DI CLASSE 2) REGISTRO DEI VERBALI CONSIGLIO DI CLASSE E INTERCLASSE 3) DOCUMENTI DI PROGRAMMAZIONE DIDATTICA 4) DOCUMENTI RELATIVI ALL'HANDICAP IN CLASSE 5) CERTIFICATI MEDICI ALLIEVI DELLA CLASSE 6) CORRISPONDENZA CON LE FAMIGLIE 7) REGISTRO PERSONALE 8) ELABORATI DEI PROPRI ALLIEVI	Aula docenti	Armadio e cassettiera	Registro elettronico Archivio assenze e voti
CS	COLLABORATORE SCOLASTICO	1) FOTOCOPIA DI DOCUMENTI PERSONALI 2) ESECUZIONE PULIZIA LOCALI SEGRETERIA / ARCHIVI	Locale fotocopie Segreteria Archivio	Fotocopiatrice	NESSUNO

Il Ministero dell'Istruzione, mediante il Regolamento dei dati sensibili e giudiziari (D.M. 305 del 07/12/2006), ha identificato in maniera precisa quali trattamenti dei dati sono consentiti all'interno di una istituzione scolastica. Per fare questo ha utilizzato il sistema delle **SCHEDE,** indicando, in ciascuna di esse, le tipologie di dati sensibili e giudiziari e di operazioni su di essi indispensabili per la gestione del sistema dell'Istruzione in un particolare comparto della stessa.
Preventivamente ha però individuato, all'Art. 2, dei limiti oggettivi entro i quali rimanere anche in caso di operazioni legittime su dati sensibili o giudiziari, infatti tutti i dati sensibili e giudiziari individuati dal regolamento in oggetto possono essere trattati previo verifica della loro:

PERTINENZA
Cioè i dati personali raccolti devono essere riferibili perfettamente all'interessato ed alla finalità del trattamento, sia nella loro forma individuale che nella forma più complessa dei documenti che li contengono.

COMPLETEZZA
Cioè i dati personali devono essere raccolti nella loro interezza onde evitare errori di valutazione che possano derivare dalla loro non completezza.

INDISPENSABILITA'
Cioè assolutamente indispensabili per raggiungere lo scopo prefissato.

SCHEDA N° 1 SELEZIONE, RECLUTAMENTO, INSTAURAZIONE, GESTIONE E CESSAZIONE DEL RAPPORTO DI LAVORO

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
STATO DI SALUTE	Stato giuridico, idoneità al servizio, assunzione categoria protette, protezione maternità, igiene e sicurezza dei luoghi di lavoro, onoreficenze, assicurazioni, trattamenti assistenziali e previdenziali, denunce infortuni, malattie professionali, fruizione permessi, assenze giustificate.	Art. 112 - Instaurazione e gestione rapporti di lavoro da parte di soggetto pubblico. Art. 62 - Rilascio documenti di riconoscimento Art. 67 - Attività di controllo ed ispettive Art. 68 - Applicazione disciplina benefici economici ed altri emolumenti. Art. 70 - Obiezione di coscienza Art. 72 - Rapporti con Enti di culto Art. 73 - Supporto al collocamento e avviamento al lavoro
ADESIONE A SINDACATI	Versamento quote di iscrizione, esercizio diritti sindacali.	
CONVINZIONI RELIGIOSE	Concessione permessi e festività religiose, reclutamento docenti di religione.	
CONVINZIONI FILOSOFICHE	Svolgimento sevizio di leva come obiettore di coscienza.	
DATI GIUDIZIARI	Valutazione requisiti di ammissione, adozione di provvedimenti amministrativo-contabili.	
VITA SESSUALE	Rettificazione attribuzione di sesso	

COMUNICAZIONI DI DATI CONSENTITE

SERVIZI SANITARI COMPETENTI PER VISITE FISCALI ED ACCERTAMENTO IDONEITA' ALL'IMPIEGO;
ORGANI PREPOSTI ALLA VIGILANZA IN MATERIA DI IGIENE E SICUREZZA LUOGHI DI LAVORO (D.Lgs. 626/1994);
ENTI ASSISTENZIALI,PREVIDENZIALI ED ASSICURATIVI;
AMMINISTRAZIONI PROVINCIALI PER GLI ASSUNTI EX L. 68/1999;
ORGANIZZAZIONI SINDACALI PER GESTIONE PERMESSI E VERSAMENTO QUOTA DI ISCRIZIONE;
PUBBLICHE AMMINISTRAZIONI VERSO LE QUALI SONO ASSEGNATI I DIPENDENTI IN MOBILITA';
ORDINARIO DIOCESANO PER IDONEITA' ALL'INSEGNAMENTO DELLA RELIGIONE CATTOLICA;
ORGANI DI CONTROLLO (CORTE DEI CONTI e MEF);
AGENZIA DELLE ENTRATE ;
PRESIDENZA DEL CONSIGLIO DEI MINISTRI PER LA RILEVAZIONE ANNUALE DEI PERMESSI PER CARICHE SINDACALI ETC.

SCHEDA N° 2	GESTIONE DEL CONTENZIOSO E PROCEDIMENTI DISCIPLINARI	
DATI SENSIBILI O GIUDIZIARI	**TRATTAMENTI CONSENTITI**	**FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE**
TUTTI I DATI SENSIBILI E GIUDIZIARI LECITAMENTE TRATTATI	Tutte le attività relative alla difesa in giudizio del Ministero della Pubblica Istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro, amministrativo, penale e civile.	Art. 112 - Instaurazione e gestione rapporti di lavoro da parte di soggetto pubblico. Art. 67 - Attività di controllo ed ispettive Art. 71 - Attività sanzionatoria e di tutela

COMUNICAZIONI DI DATI CONSENTITE

MINISTERO DEL LAVORO PER SVOLGIMENTO TENTATIVI OBBLIGATORI DI CONCILIAZIONE;
ORGANI ARBITRALI PER SVOLGIMENTO PROCEDURE ARBITRALI INDICATE NEI CCNL;
AVVOCATURA DELLO STATO PER DIFESA E CONSULENZA;
MAGISTRATURA E ORGANI DI POLIZIA GIUDIZIARIA;
LIBERI PROFESSIONISTI A FINI DI PATROCINIO E CONSULENZA, INCLUSI QUELLI DI CONTROPARTE.

SCHEDA N° 3	ORGANISMI COLLEGIALI E COMMISSIONI ISTITUZIONALI	
DATI SENSIBILI O GIUDIZIARI	**TRATTAMENTI CONSENTITI**	**FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE**
TUTTI I DATI SENSIBILI E GIUDIZIARI LECITAMENTE TRATTATI	Attivazione degli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero dell'Istruzione e dell'ordinamento scolastico.	Art. 65 - pubblicità dell'attività di organi. Art. 95 - dati sensibili e giudiziari relativi alle finalità di istruzione e di formazione in ambito scolastico.

COMUNICAZIONI DI DATI CONSENTITE

NESSUNA, ATTIVITA' INTERNA ALL'ISTITUZIONE SCOLASTICA.

SCHEDA N° 4 ATTIVITA' PROPEDEUTICHE ALL'AVVIO DELL'ANNO SCOLASTICO

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
ORIGINI RAZZIALI ED ETNICHE	Per tutti quegli atti tesi a favorire l'integrazione degli ALLIEVI di nazionalità non italiana.	Art. 68 - Applicazione disciplina benefici economici ed altri emolumenti. Art. 73 - Supporto al collocamento e avviamento al lavoro Art. 86 - Tutela maternità, disincentivazione uso sostanze psicotrope, integrazione diversamente abili, volontariato. Art. 95 - dati sensibili e giudiziari relativi alle finalità di istruzione e di formazione in ambito scolastico.
CONVINZIONI RELIGIOSE	Per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento.	
STATO DI SALUTE	Per assicurare l'erogazione del sostegno agli ALLIEVI diversamente abili e per la composizione delle classi	
DATI GIUDIZIARI	Per assicurare il diritto allo studio a soggetti detenuti, o qualora l'Autorità Giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno o ALLIEVI che abbiano commesso reati.	

COMUNICAZIONI DI DATI CONSENTITE

ENTI LOCALI PER LA FORNITURA DI SERVIZI;
GESTORI PUBBLICI E PRIVATI DI SERVIZI DI ASSISTENZA AGLI ALLIEVI E DI SUPPORTO;
AUSL ED ENTI LOCALI PER FUNZIONAMENTO GRUPPI DI LAVORO HANDICAP.

SCHEDA N° 5 ATTIVITA' EDUCATIVA, DIDATTICA E FORMATIVA, DI VALUTAZIONE

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
ORIGINI RAZZIALI ED ETNICHE	Per tutti quegli atti tesi a favorire l'integrazione degli ALLIEVI di nazionalità non italiana.	Art. 68 - Applicazione disciplina benefici economici ed altri emolumenti. Art. 73 - Supporto al collocamento e avviamento al lavoro Art. 86 - Tutela maternità, disincentivazione uso sostanze psicotrope, integrazione diversamente abili, volontariato. Art. 95 - dati sensibili e giudiziari relativi alle finalità di istruzione e di formazione in ambito scolastico.
CONVINZIONI RELIGIOSE	Per garantire la libertà di credo religioso.	
STATO DI SALUTE	Per assicurare l'erogazione del servizio di refezione scolastica, del sostegno agli ALLIEVI diversamente abili, dell'insegnamento domiciliare ed ospedaliero, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate ed ai viaggi di istruzione.	
DATI GIUDIZIARI	Per assicurare il diritto allo studio a soggetti detenuti.	
CONVINZIONI POLITICHE	Per la costituzione ed il funzionamento delle Consulte e delle Associazioni di studenti e dei genitori.	
DATI SENSIBILI IN GENERALE	In generale per le attività di valutazione periodica e finale, per le attività di orientamento e per la compilazione della certificazione delle competenze.	

COMUNICAZIONI DI DATI CONSENTITE

ALTRE ISTITUZIONI SCOLASTICHE STATALI E NON PER TRASMISSIONE DOCUMENTAZIONE ATTINENTE LA CARRIERA;
ENTI LOCALI PER FORNITURA SERVIZI;
GESTORI PUBBLICI E PRIVATI DI SERVIZI DI ASSISTENZA AGLI ALLIEVI E DI SUPPORTO;
ISTITUTI DI ASSICURAZIONE PER DENUNCIA INFORTUNI E CONNESSA R.C.;
ALL'INAIL PER LA DENUNCIA INFORTUNI;
AUSL ED ENTI LOCALI PER FUNZIONAMENTO GRUPPI DI LAVORO HANDICAP;
AZIENDE, IMPRESE ED ALTRI SOGGETTI PUBBLICI O PRIVATI PER STAGES.

SCHEDA N° 6	SCUOLE NON STATALI	
DATI SENSIBILI O GIUDIZIARI	**TRATTAMENTI CONSENTITI**	**FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE**
FASCICOLI PERSONALI DI DOCENTI E ALLIEVI	Per rendere effettiva l'attività di vigilanza e controllo eseguita dall'Amministrazione centrale o periferica nei confronti delle scuole non statali parificate.	Art. 67 - Attività di controllo ed ispettive

SCHEDA N° 7	RAPPORTI SCUOLA-FAMIGLIA, GESTIONE DEL CONTENZIOSO	
DATI SENSIBILI O GIUDIZIARI	**TRATTAMENTI CONSENTITI**	**FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE**
TUTTI I DATI SENSIBILI E GIUDIZIARI LECITAMENTE TRATTATI	Tutte le attività relative alla instaurazione del contenzioso (reclami, ricorsi, esposti, provvedimenti disciplinari, ispezioni, citazioni, denunce etc.) con gli ALLIEVI e le famiglie e tutte le attività di difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado.	Art. 67 - Attività di controllo ed ispettive Art. 71 - Attività sanzionatoria e di tutela

VII. LE MISURE DI SICUREZZA GLOBALI

La Legge, dapprima con il Decreto Legislativo 196/2003 e poi con il Regolamento UE 2016/679 definisce con il termine "misure di sicurezza", una serie di prescrizioni tecniche indispensabili affinché il trattamento dei dati personali, eseguito mediante l'impiego di apparecchiature elettroniche, sia sicuro.
Mentre la grande maggioranza di dette misure è (almeno fino alla prossima entrata in vigore di una normativa europea che aggiorni anche queste voci) positivamente indicata nel c.d. "Disciplinare Tecnico – Allegato B" del Codice della Privacy del 2003, molte altre indicazioni sono più generali e appartengono ad un metodo di lavoro organizzato secondo ragionevolezza e buona fede. All'interno dell'azienda è stato implementato il REGOLAMENTO PER L'USO DI INTERNET E DELLA POSTA ELETTRONICA, rivolto al personale dipendente e a tutti coloro che collaborano, pur in assenza di un rapporto di lavoro subordinato, nel momento in cui utilizzano le attrezzature informatiche aziendali.
É innanzitutto un aiuto per l'uso consapevole e diligente delle risorse informatiche messe a disposizione (postazioni di lavoro, dispositivi portatili, posta elettronica) evitando comportamenti che possono innescare problemi o minacce alla sicurezza del sistema. Informa inoltre delle misure di tipo organizzativo e tecnologico adottate e dei controlli che potrebbero essere effettuati, sempre nel rispetto della libertà e della dignità dei lavoratori.

USO DI INTERNET DA PARTE DEI SOGGETTI DEL TRATTAMENTO

Il corretto utilizzo di internet rappresenta uno dei punti cardini per la sicurezza dell'infrastruttura informatica entro la quale si effettua il trattamento dei dati.
Uno dei momenti più critici è quello del "download" (scaricamento) di software o dati al di fuori dai casi espressamente previsti e consentiti dal Titolare del trattamento.
L'Autorizzato al trattamento dei dati mediante utilizzo di apparecchiature informatiche, deve astenersi dal compiere "download" non autorizzati onde prevenire situazioni critiche riconducibili a due fattispecie da evitare:

<u>"DOWNLOAD" INVOLONTARIO DI SOFTWARE CHE POSSA ESPORRE LA RETE A RISCHIO DI INTRUSIONI O DI DANNO CAGIONATO DA SOFTWARE RICONDUCIBILE A QUANTO PREVISTO DALL'ART. 615 QUINQUIES DEL CODICE PENALE (VIRUS INFORMATICI)</u>

Il "download" incontrollato molto frequentemente mina le misure di sicurezza adottate a protezione della rete. Le conseguenze tipiche di tale comportamento sono: L'apertura di un varco sul dispositivo firewall che agevoli l'accesso indebito alla rete da parte di soggetti non autorizzati; Il danneggiamento dei dispositivi operato da virus informatici.

<u>"DOWNLOAD" DI DATI CHE POSSANO ESSERE CATALOGATI COME "PERSONALI" O "PARTICOLARI" IN MANIERA INCONSAPEVOLE DA PARTE DEL TITOLARE DEL TRATTAMENTO</u>

Il "download" incontrollato può riguardare non solo "maleware" (cioè software che abbia mire dannose per la rete) bensì anche dati personali o addirittura sensibili che si troveranno a risiedere su elaboratori elettronici in maniera non consapevole e quindi verranno trattati, con ogni probabilità, in maniera inadeguata.

USO DELLA POSTA ELETTRONICA DA PARTE DEI SOGGETTI DEL TRATTAMENTO

Al "download" di software o dati da internet è assimilabile la consultazione <u>non</u> remota della posta elettronica. La rete pertanto sarà configurata in modo da impedire ai soggetti del trattamento la configurazione di software di posta (Outlook, Eudora etc.) che comportino lo scaricamento dei dati sui propri elaboratori. Se la consultazione della posta elettronica privata è consentita, essa avverrà mediante accesso remoto alla casella mail tramite browser (Internet Explorer, Netscape Navigator etc.).

USO DEL FAX DA PARTE DEI SOGGETTI DEL TRATTAMENTO

I documenti in ingresso, contenenti dati personali, che dovessero pervenire via FAX, devono essere trattati con particolare cura, affinché non restino a disposizione di soggetti non autorizzati. L'Autorizzato della gestione dei FAX deve vigilare sulla corretta esecuzione della procedura di smistamento.

DISTRUZIONE DI DOCUMENTI DA PARTE DEI SOGGETTI DEL TRATTAMENTO

I documenti cartacei contenenti dati personali che, a qualsiasi titolo (dismissione di archivi, errori di scrittura, copie ridondanti etc.) debbano essere eliminati, saranno resi illeggibili dal soggetto Autorizzato mediante l'uso di un distruggidocumenti o di altro metodo parimenti idoneo.

GESTIONE DELLA POSTA CARTACEA DA PARTE DEI SOGGETTI DEL TRATTAMENTO

La posta cartacea viene raccolta dall'Autorizzato in servizio in quel momento presso la portineria / reception ed immediatamente smistata verso gli uffici.
All'atto dell'apertura tutti i documenti contenenti dati personali devono essere smistati senza ritardi a cura del personale del protocollo stesso.
Il Titolare del trattamento determina gli Autorizzati espressamente autorizzati, quali responsabili della tenuta del protocollo e della visione dei contenuti delle missive.
La posta elettronica viene "scaricata" da ciascun Autorizzato e, se stampata, segue lo stesso procedimento previsto per la posta cartacea.
Le lettere arrivate per posta che presentino all'esterno l'indicazione "RISERVATO" o altre formule atte a qualificarle come contenenti documenti di tipo particolare, non possono essere aperte dagli Autorizzati della gestione del protocollo ma devono immediatamente essere consegnati all'attenzione del Titolare del trattamento il quale provvederà alla loro custodia ed all'inoltro, o a quella del destinatario in persona.

Si rammenta che l'Art. 616 Codice Penale vieta la Violazione, sottrazione e soppressione di corrispondenza:

Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prender cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero in tutto o in parte la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da € 31,00 a € 516,00
[omissis]

VIII. MISURE DI SICUREZZA CONTRO IL RISCHIO DI DISTRUZIONE O PERDITA DI DATI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o di perdita, il Titolare del trattamento dei dati stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati. Tale periodicità tuttavia non può essere superiore alla settimana.
I criteri debbono essere stabiliti dal Titolare del trattamento in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Procedura di esecuzione del Back-up
Il Titolare del trattamento si deve preoccupare dell'esecuzione della procedura di back-up (salvataggio degli archivi).
Il Responsabile della procedura di Back-Up deve essere formato affinché sia totalmente indipendente nell'eseguire i passi tecnici necessari per l'attuazione del salvataggio delle copie degli archivi informatici contenenti dati personali.
La procedura di Back-Up deve avvenire in maniera completamente automatizzata senza bisogno dell'intervento da parte dell'operatore al fine di escludere tutte le ipotesi di dimenticanza e imperizia dell'attuazione del procedimento.

Il Titolare del trattamento è responsabile della custodia e della conservazione di supporti utilizzati per il *back up* dei dati.
Essi devono essere custoditi in modo da scongiurare il più possibile le aggressioni da:

- Agenti chimici;
- Fonti di calore;
- Campi magnetici;
- Intrusione ed atti vandalici;
- Incendio;

- Allagamento;
- Furto.

L'accesso ai supporti utilizzati per il *back up* dei dati è limitato per ogni banca dati al Titolare del trattamento della sicurezza dei dati ed all'Autorizzato al trattamento di competenza.

Se il Titolare del trattamento decide che i supporti per le copie di *back up* delle banche di dati trattate non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto, annullando e rendendo illeggibili le informazioni in esso contenute.
È compito del Titolare del trattamento assicurarsi che in nessun caso vengano lasciate copie di *back up* delle banche di dati trattate, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese illeggibili le informazioni in esso registrate.
I dati memorizzati sui supporti di back-up, nonché sui dispositivi mobili di archiviazione, devono risiedere sugli stessi in forma non-intellegibile; perché questo avvenga è necessario prevedere l'installazione di software di crittografia dei dati che impediscano, in caso di furto o smarrimento accidentale di questi supporti, la lettura da parte di chicchessia non autorizzato.
Con periodicità almeno semestrale viene verificato il corretto funzionamento della procedura di back-up simulando un ripristino totale dei dati.

IX. ALTRE MISURE DI SICUREZZA

Le regole vigenti vietano a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Titolare di dati oggetto del trattamento;
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Titolare, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Titolare, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- Consegnare a persone non autorizzate dal Titolare, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.

Il Titolare deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.
In linea di massima sono autorizzate all'accesso ai locali esclusivamente quelle persone incaricate del trattamento alle quali, il Titolare, concede l'accesso ai luoghi fisici mediante la consegna di un badge o di una chiave, nonché l'accesso agli ambiti informatici mediante la consegna di idonei criteri di accesso.

Il Titolare deve informare con una comunicazione scritta l'Autorizzato, dell'ufficio dei compiti che gli sono stati affidati e deve provvedere a formarlo affinché le mansioni indicate nella lettera gli siano familiari.

ASSEGNAZIONE NOMI UTENTE
Il Titolare deve definire le modalità di assegnazione dei nomi identificativi per consentire a ciascun Autorizzato al trattamento di accedere ai sistemi di trattamento delle banche di dati.
Non sono ammessi nomi identificativi di gruppo, con la sola eccezione dei pochi identificativi assegnati per l'amministrazione di sistema, relativamente ai sistemi operativi che prevedono un unico livello di accesso.
In ogni caso, un codice identificativo assegnato ad un Autorizzato al trattamento deve essere annullato se l'Autorizzato al trattamento ha dato le dimissioni.

ASSEGNAZIONE DELLE PASSWORD
Il Titolare deve definire le modalità di assegnazione delle *password* e decidere che ogni utente Autorizzato al trattamento possa modificare autonomamente la propria *password* di accesso.
In questo caso la modifica richiede che venga data comunicazione al Custode della *password* e al Responsabile del trattamento (se diverso dal Custode delle *password*).
Le password saranno composte da almeno 8 caratteri e non dovranno contenere elementi immediatamente riconducibili ai proprietari delle stesse.

SICUREZZA DELLE TRASMISSIONI DATI
Al fine di garantire la sicurezza delle trasmissioni dei dati su rete pubblica, il Titolare stabilisce le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione su ogni sistema collegato in rete pubblica.
I criteri debbono essere definiti dal Titolare in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI
Il Documento è costantemente aggiornato ad opera del Titolare circa ogni variazione dell'elenco degli Autorizzati del trattamento autorizzati al trattamento dei dati personali.
In particolare, in caso di trattamento automatizzato di dati, per ogni Autorizzato al trattamento deve essere indicato lo USER ID assegnato.

In caso di dimissioni di un Autorizzato al trattamento o di revoca delle autorizzazioni al trattamento dei dati, il Titolare deve darne immediata comunicazione affinché si provveda a disattivare la possibilità di accesso al sistema per il soggetto in questione.
Al Titolare è affidato il compito di verificare, ogni anno, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati, oltre al compito di redigere e di aggiornare ad ogni variazione i permessi di accesso per ogni Autorizzato al trattamento autorizzato.
In particolare, per ogni Autorizzato al trattamento e per ogni banca dati debbono essere indicati i privilegi assegnati tra seguenti:

I. Inserimento dei dati;
II. Lettura e stampa dei dati;
III. Modifica di dati;
IV. Cancellazione di dati.

X. MANUTENZIONE DELLE APPARECCHIATURE

Al Titolare al trattamento dei dati è affidato il compito di verificare ogni anno la situazione delle apparecchiature installate con cui vengono trattati i dati, delle apparecchiature periferiche e, in particolare, dei dispositivi di collegamento con le reti pubbliche.

La verifica ha lo scopo di controllare l'affidabilità del sistema per quanto riguarda:

- La sicurezza dei dati trattati;
- Il rischio di distruzione o di perdita;
- Il rischio di accesso non autorizzato o non consentito, tenendo conto anche dell'evoluzione tecnologica.

Al Titolare è affidato il compito di verificare ogni anno la situazione dei Sistemi Operativi installati sulle apparecchiature con le quali vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi per quanto riguarda:

- La sicurezza dei dati trattati;
- Il rischio di distruzione o di perdita;
- Il rischio di accesso non autorizzato o non consentito,

tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei Sistemi operativi utilizzati;
- Segnalazioni di *Patch*, *Fix* o *System-Pack* per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

Nel caso in cui esistano rischi evidenti il Titolare deve prendere gli opportuni provvedimenti allo scopo di assicurarne il corretto trattamento dei dati in conformità alle norme in vigore.

Al Titolare è affidato il compito di verificare ogni anno la situazione delle applicazioni installate sulle apparecchiature con le quali vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità del *software* applicativo, per quanto riguarda:

- La sicurezza dei dati trattati;
- Il rischio di distruzione o di perdita;
- Il rischio di accesso non autorizzato o non consentito,

tenendo conto in particolare della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.
Nel caso in cui esistano rischi evidenti il Titolare deve prendere gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

XI. IL DATA BREACH

Una violazione dei dati personali (c.d. *data breach*) può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali ed immateriali alle persone fisiche coinvolte.
Alcuni esempi che possiamo fare di questi danni sono: la perdita del controllo dei dati personali che li riguardano o la limitazione dei loro diritti, casi di discriminazione, furto o usurpazione d'identità, perdite finanziarie connesse alla sottrazione delle credenziali dell'home banking, decifratura non autorizzata delle forme di pseudonimizzazione attuate, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale e d'ufficio o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.
Questo paragrafo si prefigge lo scopo di indicare, al Titolare del trattamento dei dati, le opportune modalità di gestione del *data breach*, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016 (Considerando n. 85,86,87,88 ed Artt. 33 e 34) e nella *Guidelines on personal data breach notification under Regulation 2016/679 – article 29 data protection working party*.

In questo parte del documento si sintetizzano le regole per garantire il rispetto dei principi esposti e la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione del *data breach*, sotto i diversi aspetti relativi a:

- modalità di segnalazione al Titolare da parte di chi venga a conoscenza della violazione
- modalità e profili di segnalazione all'Autorità Garante
- valutazione dell'evento accaduto
- eventuale comunicazione agli interessati

Ogni operatore autorizzato a trattare i dati personali, qualora venga a conoscenza di un potenziale caso di *data breach,* avvisa tempestivamente il Titolare del trattamento.
Ai fini di una corretta classificazione dell'episodio, il Titolare utilizzerà lo schema di scenario di *data breach*, riportato alle pagine seguenti.

Sulla scorta delle determinazioni raggiunte, il Titolare predispone l'eventuale comunicazione all'Autorità Garante, a propria firma, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.
E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il Titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi).
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del Titolare.

Nel caso in cui dal *data breach* possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.
Il Titolare del trattamento predispone l'eventuale comunicazione agli interessati da inviarsi nei tempi e nei modi che lo stesso, individuerà come più opportuna come specificato nell'art. 34 del G.D.P.R. e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.

La comunicazione deve comprendere almeno:

• nome e recapiti del Titolare;
• le probabili conseguenze della violazione dei dati;
• eventuali misure adottate dal Titolare per porre rimedio o attenuare l'infrazione.

L'adeguatezza di una comunicazione è determinata non solo dal contenuto del messaggio, ma anche dalle modalità di effettuazione. Le linee guida, sulla base dell'art. 34, ricordano che devono sempre essere privilegiate modalità di comunicazione diretta con i soggetti interessati (quali email, SMS etc.).

Si è detto, ai paragrafi precedenti, che ogniqualvolta il Titolare si trovi ad affidare il trattamento di dati ad un soggetto terzo/responsabile del trattamento, è tenuto a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di *data breach* sia inclusa nel suddetto contratto; ciò al fine di obbligare il responsabile ad informare il Titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di *data breach*.
Ad ogni responsabile del trattamento deve essere comunicato il contatto del Titolare al quale effettuare la predetta segnalazione.
La comunicazione deve avvenire senza ingiustificato ritardo, per "ingiustificato ritardo" si considera la notizia pervenuta al Titolare al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del responsabile.
Il Titolare effettua una valutazione dell'evento avvalendosi, nel caso, del gruppo privacy del soggetto esterno.
Ai fini di una corretta classificazione dell'episodio il Titolare utilizzerà lo schema di scenario di *data breach* di seguito riportato.
Pertanto, sulla scorta delle determinazioni raggiunte, il Titolare predispone l'eventuale comunicazione all'Autorità Garante, a sua firma, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.
E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il Titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del referente privacy del soggetto obbligato.
Rimane salva la possibilità che sia il responsabile esterno del trattamento ad effettuare una notifica per conto del Titolare del trattamento, se il Titolare del trattamento ha rilasciato specifica autorizzazione al responsabile, all'interno del suddetto contratto. Tale notifica deve essere fatta in conformità con gli articoli 33 e 34 del G.D.P.R..
La responsabilità legale della notifica rimane in capo al Titolare del trattamento nella persona del Dirigente Scolastico.
Al fine di eseguire la valutazione dell'obbligatorietà o meno della notifica all'Autorità Garante dei data breach e di supportare i soggetti coinvolti nella procedura, vengono illustrati alcuni scenari di possibili violazioni di dati personali.

TIPO DI VIOLAZIONE (BREACH)	DEFINIZIONE	SOGLIA DI SEGNALAZIONE	ESEMPI (segnalazione SI)	CONTROESEMPI (segnalazione NO)
DISTRUZIONE	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del Titolare. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	Dati non recuperabili o provenienti da procedure non ripetibili Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi	Guasto non riparabile dell'hard disk contenente uno o più referti che, in violazione al regolamento, erano salvati localmente Incendio di archivio cartaceo Distruzione di documenti originali	Rottura di una chiavetta USB o di un hard disk che non contiene dati personali originali (in unica copia) Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo

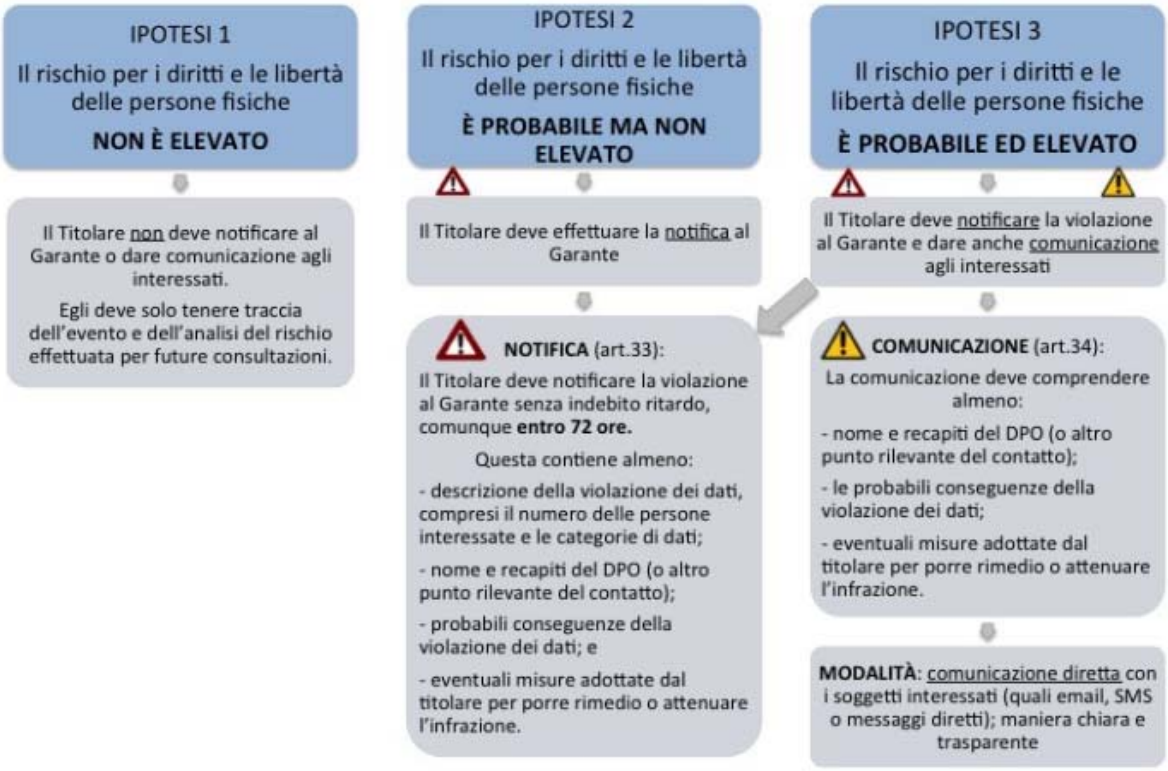
PERDITA	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del Titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	Dati non recuperabili relativi a più utenti, o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi	Smarrimento di chiavetta USB contenente dati originali Smarrimento di fascicolo cartaceo del personale o dell'utente	Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa
MODIFICA	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	Modifiche sistematiche su più casi Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi	Guasto tecnico che altera parte dei contenuti di un sistema, compromettendo anche i backup Azione involontaria, o fraudolenta, di un utente che porta alla alterazione di dati in modo non tracciato e irreversibile	Guasto tecnico che altera parte dei contenuti di un sistema, rilevato e sanato tramite operazioni di recovery Azione involontaria di un utente che porta alla alterazione di dati tracciata e reversibile Modifica di un documento non ancora validato dal proprio autore.
DIVULGAZIONE NON AUTORIZZATA	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Malfunzionamento del sistema di differenziazione delle credenziali Consegna di un CD con dati di un utente ad altra struttura senza autorizzazione	Un dipendente sul proprio sistema seleziona l'utente Mario Rossi ma interviene sull'utente Luca Bianchi., inserisce i dati e li invia al gestionale. Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet Trasmissione non

				autorizzata di un documento non ancora validato dal proprio autore.

ACCESSO NON AUTORIZZATO	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche Autorizzati dal Titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema.	Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi Accesso non autorizzata di un documento non ancora validato dal proprio autore.
INDISPONIBILITA' TEMPORANEA DEL DATO	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup Cancellazione accidentale dei dati da parte di una persona non autorizzata Perdita della chiave di decrittografia di dati crittografati in modo sicuro irraggiungibilità di un sito di stoccaggio delle cartelle cliniche poste in montagna per isolamento neve	Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso

Un *data breach*, quindi, non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, un incidente (es. un incendio o una calamità naturale), nella semplice perdita di un dispositivo mobile di archiviazione (es.

chiavetta USB, disco esterno), nella sottrazione di documenti con dati personali (es. furto di un notebook di un dipendente).
I casi di *data breach* per le casistiche già descritte si estendono dai dati digitali, ai documenti cartacei o su altri supporti analogici.
La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato *data breach,* ma è considerato un normale errore procedurale.
Al fine di schematizzare ancora meglio lo schema del ragionamento prendiamo in prestito, dallo studio legale Delli Ponti, questo diagramma:



La segnalazione di un data breach all'Autorità Garante deve contenere alcune informazioni fondamentali.
Di seguito le riportiamo per esteso (verificare sul sito del Garante la presenza di modulistica ad hoc):

1. Titolare che effettua la comunicazione:
   a. Denominazione o ragione sociale:
   b. Sede del Titolare:
   c. Persona fisica addetta alla comunicazione:
   d. Funzione rivestita:
   e. Indirizzo email per eventuali comunicazioni:
   f. Recapito telefonico per eventuali comunicazioni:

2. Natura della comunicazione:
   a. Nuova comunicazione (inserire contatti per eventuali chiarimenti, se diversi da quelli sub 1.):
   b. Seguito di precedente comunicazione (inserire numero di riferimento):
   b.1. Inserimento ulteriori informazioni sulla precedente comunicazione:
   b.2. Ritiro precedente comunicazione (inserire le ragioni del ritiro):
3. Breve descrizione della violazione di dati personali:

4. Quando si è verificata la violazione di dati personali?
   a. Il …
   b. Tra il ….. e il …..
   c. In un tempo non ancora determinato

d. È possibile che sia ancora in corso

5. Dove è avvenuta la violazione dei dati? (Specificare se smarrimento di dispositivi o supporti)

6. Modalità di esposizione al rischio:
   a. tipo di violazione:
   a.1. lettura (presumibilmente i dati non sono stati copiati)
   a.2. copia (i dati sono ancora presenti sui sistemi del Titolare)
   a.3. alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
   a.4. cancellazione (i dati non sono più sui sistemi del Titolare e non li ha neppure l'autore della violazione)
   a.5. furto (i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione)
   a.6. altro [specificare]
   b. dispositivo oggetto della violazione:
   b.1. computer
   b.2. dispositivo mobile
   b.3. documento cartaceo
   b.4. file o parte di un file
   b.5. strumento di backup
   b.6. rete
   b.7. altro [specificare]

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

8. Quante persone sono state colpite dalla violazione di dati personali?
   a. [numero esatto] persone
   b. Circa [numero] persone
   c. Un numero (ancora) sconosciuto di persone

9. Che tipo di dati sono coinvolti nella violazione?
   a. Dati anagrafici
   b. Numeri di telefono (fisso o mobile)
   c. Indirizzi di posta elettronica
   d. Dati di accesso e di identificazione (user name, password, customer ID, altro)
   e. Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
   f. Altri dati personali (sesso, data di nascita/età, …), dati sensibili e giudiziari
   g. Ancora sconosciuto
   h. Altro [specificare]

10. Livello di gravità della violazione di dati personali (secondo le valutazioni del Titolare):
   a. Basso/trascurabile
   b. Medio
   c. Alto

11. Misure tecniche e organizzative applicate ai dati colpiti dalla violazione:

12. La violazione è stata comunicata anche a contraenti (o ad altre persone interessate)?
   a. Sì, è stata comunicata il ….
   b. No, perché [specificare]

13.Qual è il contenuto della comunicazione ai contraenti (o alle altre persone interessate)? [riportare il testo della notificazione]

14. Quale canale è utilizzato per la comunicazione ai contraenti (o alle altre persone interessate)?

15. Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

16. La violazione coinvolge contraenti (o altre persone interessate) che si trovano in altri Paesi EU?
   a. No

b. Si

17. La comunicazione è stata effettuata alle competenti autorità di altri Paesi EU?
    a. No
    b. Si, (specificare)

Come accade per tutti i sistemi basati sul concetto di "rischio" e di "valutazione del rischio", la documentazione degli episodi che hanno determinato un danno (violazione dei dati – data breach) è fondamentale al fine di adottare precauzioni (tecniche o comportamentali) che possano scongiurare il verificarsi nuovamente di quell'episodio.
L'Art. 33 del G.D.P.R. pone l'attenzione su questa esigenza, il metodo migliore per adempiere a questa regola ma anche per poter comprovare, in caso di ispezione, tale adempimento consiste nella tenuta di un registro dei data breach (già previsto dal Garante con provvedimento 161 del 04 Aprile 2013) che contenga, per ciascun episodio, queste informazioni essenziali:

1. Dettagli relativi alla violazione (cause, luogo, tipologia di dati violati);
2. Effetti e conseguenze della violazione;
3. Piano di intervento predisposto dal Titolare;
4. Le motivazioni delle decisioni assunte a seguito del data breach nei casi in cui:
    a. Il Titolare ha deciso di non procedere alla notifica;
    b. Il Titolare ha ritardato nella procedura di notifica;
    c. Il Titolare ha deciso di non notificare il data breach agli interessati.

XII. VALUTAZIONE DEI RISCHI INCOMBENTI SUI DATI PERSONALI OGGETTO DI TRATTAMENTO

Il G.D.P.R. predilige, piuttosto che un approccio basato sulla protezione dell'utenze, uno "risk-based", cioè basato sul concetto di "rischio" circa il verificarsi di un evento che possa determinare una violazione dei dati.
Il Considerando 75 definisce il rischio in questo modo: "*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*".

Tale approccio prevede l'obbligo di una analisi del rischio del trattamento, al fine della valutazione delle misure di sicurezza che il Titolare ritiene di dover adottare per ridurre l'eventuale rischio in termini di probabilità di accadimento e di gravità del danno atteso.

Le tabelle che seguono propongono una valutazione per "categorie" di rischi riferibili a:

- CATTIVO COMPORTAMENTO DEGLI OPERATORI E DI TERZI
- MALFUNZIONAMENTO DELLE APPARECCHIATURE
- EVENTI FISICI ED ATMOSFERICI
- CONNESSIONE AD INTERNET

EVENTI DANNOSI IN SEGUITO A CATTIVO COMPORTAMENTO DEGLI OPERATORI O DI SOGGETTI TERZI

Descrizione del rischio	Probabilità dell'evento	Trattamento interessato	Misura di sicurezza adottata	Tipologia della misura	Livello di adeguatezza
Danneggiamento volontario	BASSA	TUTTI	Vigilanza sugli operatori	PREVENTIVA / DI CONTENIMENTO	Adeguata
Furto	BASSA	TUTTI	Vigilanza sugli operatori Installazione di un sistema antifurto o di sistemi anti-intrusione nei locali ove sono tenuti i dati. Adozione di tecniche di cifratura dei dati	PREVENTIVA / DI CONTRASTO	Adeguata
Uso non autorizzato di supporti di memoria	ALTA	TRATTAMENTI INFORMATICI	Vigilanza sugli operatori e configurazione di utenze non amministrative. Adozione di tecniche di cifratura dei dati	PREVENTIVA	Adeguata
Errore del personale operativo	MEDIA	TUTTI	Vigilanza sugli operatori ed organizzazione corsi di formazione	PREVENTIVA	Adeguata
Errore di manutenzione	MEDIA	TRATTAMENTI INFORMATICI	Impiego di personale specializzato	PREVENTIVA	Adeguata
Uso illegale di software	ALTA	TRATTAMENTI INFORMATICI	Vigilanza sugli operatori e configurazione di utenze non amministrative	PREVENTIVA	Adeguata
Accesso non autorizzato alla rete	MEDIA	TRATTAMENTI INFORMATICI	Configurazione di utenze protette da password	PREVENTIVA	Parzialmente adeguata
Indirizzamento non corretto della posta elettronica	MEDIA	TRATTAMENTI INFORMATICI	Vigilanza sul personale e formazione dello stesso	PREVENTIVA	Adeguata
Sottrazione di credenziali di autenticazione	MEDIA	TRATTAMENTI INFORMATICI	Configurazione di un sistema di cambio periodico della password e di disattivazione in caso di prolungato non impiego dell'utenza	PREVENTIVA	Parzialmente adeguata
Visione da parte di soggetti non autorizzati di dati cartacei dopo la loro eliminazione	ALTA	TRATTAMENTI CARTACEI	Impiego di un distruggidocumenti o di altro metodo per rendere illeggibili tutti i fogli contenenti dati personali	DI CONTRASTO	Adeguata
Lettura da parte di soggetti non autorizzati di dati digitali su supporti magnetici dopo la loro dismissione	MEDIA	TRATTAMENTI INFORMATICI	Impiego di un distruggi-CD o di altro metodo di annullamento dei supporti	DI CONTRASTO	Adeguata

EVENTI DANNOSI IN SEGUITO A MALFUNZIONAMENTO DELLE APPARECCHIATURE

Descrizione rischio	Probabilità dell'evento	Trattamento interessato	Misura di sicurezza adottata	Tipologia della misura	Livello di adeguatezza
Guasto hardware	MEDIA	TRATTAMENTI INFORMATICI	Continua manutenzione delle apparecchiature	PREVENTIVA / DI CONTENIMENTO	Adeguata
Linea elettrica instabile	MEDIA	TRATTAMENTI INFORMATICI	Installazione di unità di continuità elettrica stabilizzate	PREVENTIVA / DI CONTENIMENTO	Adeguata
Guasto tecnico al provider di rete	MEDIA	TRATTAMENTI INFORMATICI	Conclusione di contratti di somministrazione del servizio con provider certificati	PREVENTIVA	Adeguata
Danni sulle linee di rete	BASSA	TRATTAMENTI INFORMATICI	Certificazione realizzazione impianto secondo le regole dell'arte	PREVENTIVA	Adeguata
Guasto software	MEDIA	TRATTAMENTI INFORMATICI	Continua manutenzione delle apparecchiature	PREVENTIVA / DI CONTENIMENTO	Adeguata
Azione di virus informatici o di altro maleware	ALTA	TRATTAMENTI INFORMATICI	Installazione di un software antivirus di rete adeguato	PREVENTIVA / DI CONTRASTO /DI CONTENIMENTO	Adeguata
Spamming e tecniche di sabotaggio informatico	ALTA	TRATTAMENTI INFORMATICI	Installazione di un sistema di firewalling dimensionato sulla struttura	PREVENTIVA / DI CONTRASTO / DI CONTENIMENTO	Adeguata
Degrado delle apparecchiature	MEDIA	TRATTAMENTI INFORMATICI	Continua manutenzione e redazione di un piano di sostituzioni	PREVENTIVA	Parzialmente adeguata
Intercettazioni di informazioni di rete	MEDIA	TRATTAMENTI INFORMATICI	Installazione di un sistema di firewalling dimensionato sulla struttura e adozione di policy di rete corrette	PREVENTIVA	Parzialmente adeguata

EVENTI DANNOSI IN SEGUITO AD EVENTI FISICI ED ATMOSFERICI

Descrizione rischio	Probabilità dell'evento	Trattamento interessato	Misura di sicurezza adottata	Tipologia della misura	Livello di adeguatezza
Inondazione	BASSA	TUTTI I TRATTAMENTI	I SERVER ed in generale i dispositivi contenenti dati sono posti su supporti rialzati	DI CONTRASTO / DI CONTENIMENTO	Adeguata
Fulmine	BASSA	TRATTAMENTI INFORMATICI	Installazione di unità di continuità elettrica stabilizzate	DI CONTRASTO / DI CONTENIMENTO	Adeguata
Fuoco	BASSA	TUTTI I TRATTAMENTI	I SERVER ed in generale i dispositivi contenenti dati sono installati in locali dotati di estintore o di sistema anti-incendio	DI CONTRASTO / DI CONTENIMENTO	Adeguata
Temperatura ed umidità eccessive	MEDIA	TRATTAMENTI INFORMATICI	I SERVER ed in generale i dispositivi contenenti dati sono posti all'interno di locali chiusi	DI CONTRASTO / DI CONTENIMENTO	Adeguata
Polvere	ALTA	TRATTAMENTI INFORMATICI	I SERVER ed in generale i dispositivi contenenti dati sono posti all'interno di locali chiusi	DI CONTRASTO / DI CONTENIMENTO	Adeguata
Radiazioni elettromagnetiche	MEDIA	TRATTAMENTI INFORMATICI	I SERVER ed in generale i dispositivi contenenti dati sono posti all'interno di locali chiusi	DI CONTRASTO / DI CONTENIMENTO	Adeguata

RISCHI SPECIFICI CUI SONO SOTTOPOSTE LE RISORSE CONNESSE AD INTERNET

Descrizione del rischio	Probabilità dell'evento	Trattamento interessato	Misura di sicurezza adottata	Tipologia della misura	Livello di adeguatezza
IP SPOOFING Ovvero rischio che l'autore dell'attacco sostituisca la propria identità a quella dell'utente legittimo del sistema. Viene fatto non per generare intrusioni in senso stretto ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici come l'indirizzo IP o il mittente di E-mail	MEDIA	TRATTAMENTI INFORMATICI	Azione di protezione ottenuta dall'azione combinata di FIREWALL e SOFTWARE ANTIVIRUS	PREVENTIVA	Adeguata
PACKET SNIFFING Apprendimento di informazioni e dati presenti in un sistema tramite l'uso di appositi programmi. L'aggressore mediante questi programmi è in grado di "intercettare" password, messaggi etc.	MEDIA	TRATTAMENTI INFORMATICI	Azione di protezione ottenuta dall'azione combinata di FIREWALL e SOFTWARE ANTIVIRUS	PREVENTIVA	Adeguata
PORT SCANNING Serie programmata di tentativi di accesso ad un sistema diretti ad evidenziare, in funzione delle risposte ottenute, le caratteristiche tecniche del medesimo e, conseguentemente, le eventuali vulnerabilità	MEDIA	TRATTAMENTI INFORMATICI	Azione di protezione ottenuta dall'azione combinata di FIREWALL e SOFTWARE ANTIVIRUS	PREVENTIVA	Adeguata
HIGHJACKING Intrusione in una connessione di rete in corso, simulando di essere una macchina parte della "conversazione" di rete	MEDIA	TRATTAMENTI INFORMATICI	Azione di protezione ottenuta dall'azione combinata di FIREWALL e SOFTWARE ANTIVIRUS	PREVENTIVA	Adeguata
PASSWORD CRACKING Programmi in grado di acquisire le password nel momento in cui queste sono digitate a tastiera	MEDIA	TRATTAMENTI INFORMATICI	Azione di protezione ottenuta dall'azione combinata di FIREWALL e SOFTWARE ANTIVIRUS	PREVENTIVA	Adeguata

XIII. LA TUTELA DEI DIRITTI DEGLI INTERESSATI (PROCEDURA)

Occorre definire le modalità e le responsabilità per l'adozione di misure adeguate a fornire all'interessato tutte le informazioni da egli richieste secondo quanto previsto dalla normativa, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

La procedura è applicabile a tutte le attività di trattamento dei dati personali svolte, con particolare riferimento alla gestione di tutti gli archivi/documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati (clienti, fornitori, altri soggetti terzi, ecc.), anche con il supporto di fornitori esterni.

Le richieste degli interessati possono pervenire unicamente tramite i canali previsti nell'informativa privacy fornita e possono riguardare:

- accesso ai dati;
- rettifica dei dati;
- cancellazione dei dati (diritto all'oblio);
- limitazione del trattamento;
- portabilità dei dati;
- esercizio del diritto di opposizione;
- esercizio del diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato.

Il Titolare, in base al contenuto della richiesta, provvede di conseguenza ad adempiere alla richiesta, se basata su presupposti legittimi.
Eventuali altri casi, incluse richieste che facciano riferimento al Titolare, saranno gestiti caso per caso.
Prima di evadere la richiesta, il Titolare provvederà a verificare se la stessa è completa degli elementi essenziali per la identificazione dell'interessato e l'elaborazione di una risposta e, in caso contrario le acquisisce. In particolare si intendono "essenziali":

- nome e cognome;
- estremi di un documento in corso di validità;
- oggetto della richiesta;
- data di presentazione.

L'Unità Organizzativa o la Struttura competente per la risposta la prende in carico e la elabora. La risposta fornita all'interessato deve essere "intelligibile", concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.
La risposta all'interessato va data con lo stesso strumento utilizzato da quest'ultimo (es. email) salvo diversa indicazione dell'interessato stesso.
Il termine per la risposta all'interessato è, per tutti i diritti, di 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; è comunque necessario dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.
Qualora il Titolare verifichi la impossibilità o la non applicabilità di una risposta decide se applicare la deroga alla risposta. Tali casi sono:

- impossibilità di identificare l'interessato;
- carattere manifestamente infondato o eccessivo della richiesta inviata da parte dell'interessato, in particolare per via del carattere ripetitivo della stessa; oppure, come previsto dalla normativa, se:
- la richiesta ricade nel principio di tutela del diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria
- i dati personali sono trattati a fini di ricerca scientifica o storica
- i dati personali sono archiviati a fini meramente statistici
- i dati personali sono trattati per finalità di archiviazione nel pubblico interesse.

Nel caso in cui la richiesta debba essere respinta, la risposta dovrà contenere i motivi dell'inottemperanza e le indicazioni sulla possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

Per ogni richiesta ricevuta viene compilato il “Registro delle richieste” nel quale sono riportati gli estremi della richiesta:

- numero progressivo;
- data della richiesta;
- data di ricezione della richiesta, se diversa dalla data della richiesta;
- canale di comunicazione (email, PEC, posta comune, posta raccomandata);
- nominativo dell'interessato;
- tipo di richiesta:

    o accesso ai dati;
    o rettifica dei dati;
    o cancellazione dei dati (diritto all'oblio);
    o limitazione di trattamento;
    o portabilità dei dati;
    o esercizio del diritto di opposizione;
    o esercizio del diritto di non essere sottoposto a una decisione basata sul trattamento automatizzato;
    o altro.

- Unità organizzative / strutture coinvolte nella gestione della richiesta;
- Completezza della richiesta (SI/NO);
- Fondatezza della richiesta (SI/NO);
- Complessità della richiesta (SI/NO);
- Gestione della prima risposta: data, canale di comunicazione, oggetto;
- Oneri economici per la gestione della richiesta (in ore / persona);
- Stato della richiesta (in corso/chiusa);
- Data di chiusura della gestione della richiesta;
- Note.

Qualora la richiesta riguardi l'accesso ai dati personali, una volta confermata la completezza e la fondatezza della richiesta stessa, il Titolare con il supporto della Struttura interessata, e dopo verifica che l’ottenimento della copia possa ledere i diritti e le libertà altrui, predispone una copia dei dati personali oggetto di trattamento.
Oltre quanto indicato in precedenza, nel caso specifico, si applicano le seguenti regole:

La riposta contiene la conferma che sia o meno in corso un trattamento di dati personali che riguardano l’interessato e, in tal caso, contiene i dati personali e le seguenti informazioni:

1. le finalità del trattamento;
2. le categorie di dati personali in questione;
3. i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
4. quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
5. l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
6. il diritto di proporre reclamo a un'autorità di controllo;
7. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
8. l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;
9. qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, esistenza di garanzie adeguate relative al trasferimento.

Qualora la richiesta riguardi la rettifica dei dati, confermata la completezza e la fondatezza della richiesta stessa, il Titolare trasmette agli uffici interessati un elenco dei dati personali inesatti e/o dei dati personali incompleti, in forma scritta, preferibilmente a mezzo email. Terminate le operazioni di rettifica/integrazione, gli uffici interessati comunicano al Titolare il completamento delle attività, in forma scritta, preferibilmente a mezzo email.

Le attività di rettifica/integrazione vanno completate senza ingiustificato ritardo.
Secondo le modalità indicate, il Titolare, con il supporto degli uffici interessati, predispone la risposta alla richiesta dell'interessato.

Il Titolare, con il supporto degli uffici interessati, comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.
La risposta all'interessato contiene i nominativi di tali destinatari, qualora l'interessato lo richieda.

Qualora la richiesta riguardi la cancellazione dei dati, confermata la completezza e la fondatezza della richiesta stessa, il Titolare trasmette agli uffici interessati un elenco dei dati personali da cancellare, in forma scritta, preferibilmente a mezzo email. Terminate le operazioni di cancellazione, le funzioni competenti comunicano al Titolare stesso il completamento delle attività, in forma scritta, preferibilmente a mezzo email.
Secondo le modalità indicate, il Titolare, con il supporto degli uffici interessati, dopo aver verificato la fondatezza della richiesta predispone la risposta alla richiesta dell'interessato, in caso contrario, comunica il respingimento della richiesta.

Per valutare la fondatezza della richiesta stessa, il Titolare, verifica preliminarmente se sussiste uno dei motivi seguenti:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento per finalità di marketing diretto, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto; - i dati personali sono trattati illecitamente;
- i dati personali devono essere cancellati per adempiere ad un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetta il Titolare del trattamento;
- i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori.

Per valutare il respingimento della richiesta stessa il Titolare verifica se il trattamento dei dati è necessario per uno dei motivi seguenti:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui la cancellazione rischia di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il Titolare, con il supporto degli uffici interessati, comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali cancellazioni effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.
La risposta all'interessato contiene i nominativi di tali destinatari, qualora l'interessato lo richieda.
In particolare, se il Titolare del trattamento ha reso pubblici i dati personali oggetto della richiesta, esso è obbligata a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, per cui il Titolare stesso identifica le misure per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato e per garantire la cancellazione di qualsiasi link, copia o riproduzione dei suoi dati personali.

Qualora la richiesta riguardi la limitazione del trattamento dei dati, confermata la completezza e la fondatezza della richiesta stessa, il Titolare, trasmette agli uffici interessati un elenco dei dati personali di cui limitare il trattamento, in forma scritta, preferibilmente a mezzo email, e concorda con esse le misure per contrassegnare il dato personale in attesa di determinazioni ulteriori. Terminate le operazioni di contrassegno e limitazione del trattamento, gli uffici interessati comunicano al Titolare il completamento delle attività, in forma scritta, preferibilmente a mezzo email.
Se il Titolare del trattamento ha reso pubblici i dati personali oggetto della richiesta, essa è obbligata a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, per cui identifica le misure per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato e per garantire la cancellazione di qualsiasi link, copia o riproduzione dei suoi dati personali.

Secondo le modalità indicate, il Titolare, con il supporto degli uffici interessati, predispone la risposta alla richiesta dell'interessato.

Il Titolare, con il supporto degli uffici interessati, comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.
La risposta all'interessato contiene i nominativi di tali destinatari, qualora l'interessato lo richieda.

Se il trattamento è limitato, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
Il Titolare, con il supporto degli uffici interessati, verifica che, per i dati per i quali siano in corso delle limitazioni di trattamento, siano attuati solo i trattamenti consentiti, fino a revoca delle limitazioni.

Il Titolare, con il supporto delle funzioni competenti, identifica i termini per la revoca della limitazione richiesta e ne informa l'interessato prima che detta limitazione sia revocata.

Qualora la richiesta riguardi la portabilità dei dati, confermata la completezza e la fondatezza della richiesta stessa, il Titolare trasmette agli uffici interessati un elenco dei dati personali di cui effettuare la portabilità, in forma scritta, preferibilmente a mezzo email.
Terminate le operazioni di portabilità, gli uffici interessati comunicano al Titolare stesso il completamento delle attività, in forma scritta, preferibilmente a mezzo email. Il diritto di ottenere la portabilità dei dati non deve ledere i diritti e le libertà altrui.
Secondo le modalità indicate, il Titolare, con il supporto degli uffici interessati, predispone la risposta alla richiesta dell'interessato.
Nel caso specifico, si applicano le seguenti regole.

Per valutare la fondatezza della richiesta stessa, il Titolare, verifica se sussistano entrambe le condizioni seguenti:

- il trattamento si basi sul consenso, anche in riferimento a dati sensibili, o su un contratto;
- il trattamento sia effettuato con mezzi automatizzati.

Inoltre, sono portabili i dati personali che:

- riguardano l'interessato, e
- sono stati forniti dall'interessato a un Titolare, intendendo sia i dati forniti consapevolmente e attivamente dall'interessato (ad esempio indirizzo postale, nome utente, età), sia i dati osservati forniti dall'interessato attraverso la fruizione di un servizio o l'utilizzo di un dispositivo (ad esempio cronologia delle ricerche effettuate dall'interessato e dati relativi al traffico).

L'interessato può continuare a fruire e beneficiare del servizio offerto dal Titolare anche dopo che sia compiuta un'operazione di portabilità. La portabilità non comporta la cancellazione automatica dei dati conservati nei sistemi del Titolare, e non incide sul periodo di conservazione previsto originariamente per i dati oggetto di trasmissione.
Il diritto alla portabilità non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

I dati oggetto di portabilità sono riportati su un formato strutturato, di uso comune e leggibile da dispositivo automatico; ove possibile, tale formato dovrebbe essere interoperabile.

La richiesta dell'interessato può comprendere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro, se tecnicamente fattibile.
In tal caso, il Titolare, coinvolge le funzioni competenti per identificare le modalità per tale trasmissione diretta.
Qualora la richiesta riguardi l'esercizio del diritto di opposizione, confermata la completezza e la fondatezza della richiesta stessa, il Titolare, trasmette alle funzioni competenti un elenco dei dati personali di cui interrompere il trattamento, compresa la profilazione, in forma scritta, preferibilmente a mezzo email. Terminate le operazioni di interruzione del trattamento, le funzioni competenti comunicano al Titolare il completamento delle attività, in forma scritta, preferibilmente a mezzo email.
Secondo le modalità indicate, il Titolare, con il supporto delle funzioni competenti, predispone la risposta alla richiesta dell'interessato.

Oltre quanto indicato, nel caso specifico, si applicano le seguenti regole.
Nel contesto dell'utilizzo di servizi della società dell'informazione, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
Per valutare la fondatezza della richiesta stessa, il Titolare, verifica se la stessa riguarda dati personali che sono trattati per finalità di marketing diretto, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto, caso in cui l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità.
La richiesta è fondata anche qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.
Per valutare il respingimento della richiesta stessa, il Titolare, verifica l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici, la richiesta viene respinta se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Il Titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, inclusi il diritto di ottenere l'intervento umano (non automatizzato) da parte del Titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
Qualora la richiesta riguardi esercizio del diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, confermata la completezza e la fondatezza della richiesta stessa, secondo le modalità indicate, il Titolare, con il supporto degli uffici interessati, predispone la risposta alla richiesta dell'interessato.
Oltre quanto indicato nel caso specifico, si applicano le seguenti regole.

Per valutare il respingimento della richiesta stessa, il Titolare, verifica che la decisione sia stata presa al verificarsi di una delle seguenti condizioni:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un Titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento);
- si basi sul consenso esplicito dell'interessato.

Comunque, tranne che nel secondo caso, il Titolare, verifica che siano in atto misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del Titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
Qualora i dati personali oggetto della richiesta siano trattati da uno o più responsabili del trattamento, il Titolare del trattamento definisce contrattualmente con i responsabili del trattamento le modalità con le quali essi assicurano l’obbligo di assistere il Titolare del trattamento con misure tecniche e organizzative adeguate nel dare seguito alle richieste di esercizio dei diritti dell’interessato, di cui il Titolare del trattamento resta legalmente responsabile.

XIV. FORMAZIONE DEGLI INCARICATI

Al Titolare del trattamento dei dati è affidato il compito di verificare annualmente le necessità di formazione del personale incaricato di eseguire i compiti indicati nella lettera di incarico.
Per ogni incaricato del trattamento il Titolare, di concerto con il Responsabile della Protezione dei Dati definisce, sulla base dell'esperienza e delle sue conoscenze ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessaria una formazione specifica ulteriore e la organizza:

PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessate
CORSO DI FORMAZIONE PER SOGGETTI DEL TRATTAMENTO Oggetto : - Informazione sul contenuto e disposizioni del Regolamento UE 2016/679 - Uso delle CREDENZIALI DI ACCESSO ALLA RETE - Concetti di "IGIENE INFORMATICA" - Rilevanza legale del BACK-UP - Il Documento delle Misure a Tutela dei Dati delle Persone - Natura giuridica della "LETTERA DI INCARICO" - Analisi dei rischi collegati alle attività proprie della categoria - Organizzazione e procedure di sicurezza	TITOLARE DEL TRATTAMENTO RESPONSABILE DEL TRATTAMENTO INCARICATI DEL TRATTAMENTO COLLABORATORI DEL DIRIGENTE COORDINATORI DI PLESSO
CORSO DI FORMAZIONE PER SOGGETTI DEL TRATTAMENTO Oggetto : - Informazione sul contenuto e disposizioni del Regolamento UE 2016/679 - Cenni di diritto scolastico (potestà genitoriale, uso delle immagini etc.) - Il Documento delle Misure a Tutela dei Dati delle Persone - Natura giuridica della "LETTERA DI INCARICO" - Analisi dei rischi collegati alle attività proprie della categoria - Organizzazione e procedure di sicurezza	DOCENTI ADDETTI ALLA SICUREZZA (D.Lgs 81/08) COMMISSIONE FORMAZIONE CLASSI MEMBRI COMITATO DI VALUTAZIONE COLLABORATORI SCOLASTICI

XV. REVISIONI

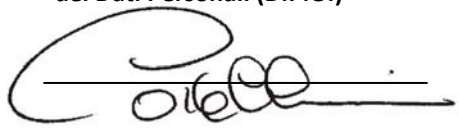
Il presente Documento delle Misure a Tutela dei Dati delle Persone, dovrà essere revisionato annualmente.

Il presente Documento delle Misure a Tutela dei Dati delle Persone è stato redatto da Luca Corbellini, di concerto con il Titolare del trattamento, in seguito all'acquisizione dell'incarico di Responsabile della Protezione dei Dati Personali (D.P.O. – R.P.D.) sulla base delle informazioni acquisite in uno o più colloqui intercorsi con il personale incaricato dal titolare del trattamento dei dati, a descrivere l'attività svolta negli uffici.
Il Responsabile della Protezione dei Dati non è responsabile per l'esattezza delle informazioni fornite non altrimenti verificabili.

Il Documento delle Misure a Tutela dei Dati delle Persone viene letto e confermato in ogni suo punto.

Data _____

Responsabile della Protezione dei Dati Personali (D.P.O.)



Titolare del trattamento

_____