CPIA 3 Sud-Milano "Maestro A. Manzi"

Viale Liguria, 7 20089 Rozzano (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 : **13/03/2019**

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.

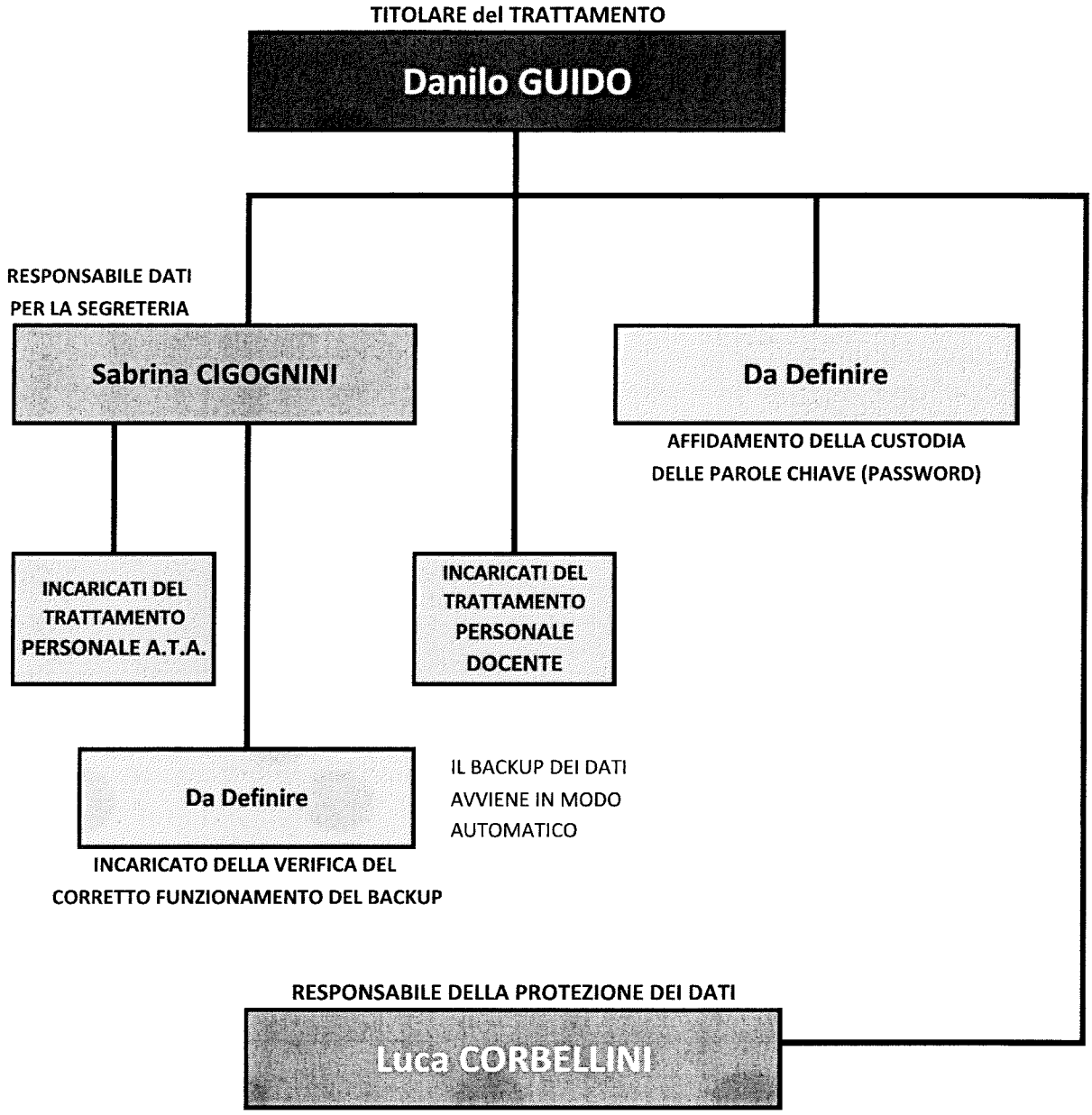
Per l'ente in oggetto le sedi in cui avviene il trattamento sono:

Tabella A

SEDE LEGALE

CPIA 3 Sud-Milano "Maestro A. Manzi"	Viale Liguria, 7, 20089 - Rozzano (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.

X	TITOLARE
S	SUPPLENTE

ORGANIGRAMMA DELLA PRIVACY (INCARICATI DEL TRATTAMENTO)

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

NOME e COGNOME	FUNZIONE	STUDENTI	DIPENDENTI	FORNITORI		PROTOCOLLO	POSTA ELETTRONICA
Antonietta CORDISCO	ASSISTENTE AMMINISTRATIVO	X	X	X		X	X
Pietro GATTULLI	ASSISTENTE AMMINISTRATIVO	X	X			X	X
Rosario NUNZIATA	ASSISTENTE AMMINISTRATIVO	X	X			X	X
Bice PAGLIUSO	ASSISTENTE AMMINISTRATIVO	X	X			X	X

NOME e COGNOME	FUNZIONE	ARCHIVIO (*)
Gianfranco FACCHINETTI	I° COLLABORATORE DEL DIRIGENTE SCOLASTICO	ALLIEVI
Giovanni MASCOTTO	RESPONSABILE DI PLESSO	ALLIEVI
Francesca GAGLIARDI	RESPONSABILE DI PLESSO	ALLIEVI
Claudia GIRARDO	RESPONSABILE DI PLESSO	ALLIEVI
Lorenzo LONGARETTI	RESPONSABILE DI PLESSO	ALLIEVI
Rita LOZZI	RESPONSABILE DI PLESSO	ALLIEVI
Maria Angela POGLIO	RESPONSABILE DI PLESSO	ALLIEVI

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

INDICE

I° SEZIONE – ANAGRAFICA, FINALITA', NORMATIVA

II° SEZIONE – REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

III° SEZIONE – VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

IV° SEZIONE – VALUTAZIONI PROGRAMMATICHE

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 RISCATTO PENSIONE E LIQUIDAZIONE	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

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	D. S.	SEGRETERIA	Danilo GUIDO
	D.S.G.A.	SEGRETERIA	Sabrina CIGOGNINI
	ASS. TECNICO	SEGRETERIA	MICROTECH S.R.L.

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.	Microtech S.R.L.,Via A. Moro,9,20090-Buccinasco(MI)	ESTERNO

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	Andrea REALI SPL Consulenza S.R.L. Via Capri, 5 27100 - Pavia (PV)	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. Giuseppe CANNONE Via Oglio, 8 27100 - Pavia (PV)	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				
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 minime di sicurezza", una serie di prescrizioni tecniche indispensabili affinché il trattamento dei dati personali, eseguito mediante l'impiego di apparecchiature elettroniche, sia minimamente sicuro.
Mentre la stragrande 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:

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.
Il momento "critico" è quello del "download" (scaricamento) di software o dati al di fuori dai casi espressamente previsti e consentiti dal Titolare del trattamento.
L'incaricato del 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:

"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)

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.

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

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 non 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 pervengano via FAX, devono essere trattati con particolare cura, affinché non restino a disposizione di soggetti non autorizzati. L'incaricato 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 incaricato 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'incaricato 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 incaricati espressamente autorizzati, quali responsabili della tenuta del protocollo e della visione dei contenuti delle missive.

La posta elettronica viene "scaricata" da ciascun incaricato 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 incaricati 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:

Art. 616 Codice Penale
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 dei dati nomina il "Responsabile della procedura di Back-Up" con espressa lettera di incarico.
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.
Le mansioni cui è soggetto il Responsabile della procedura di Back-Up sono indicate in via generale nella lettera di incarico.

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'Incaricato del 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 criptaggio 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. CRITERI PER LA TENUTA DI SUPPORTI DIGITALI REMOVIBILI

I supporti di back-up (nastri, CD, DVD, FDD etc.), nonché tutti i supporti digitali removibili (PEN DRIVE, SD etc.) contenenti dati personali, devono essere limitati al minimo nel loro numero, devono essere tenuti esclusivamente da soggetti espressamente autorizzati e, se i dati sono di natura sensibile, devono risiedere sui supporti di archiviazione in formato non intellegibile in quanto, in considerazione della loro forma, del loro peso e della loro facile portabilità, il rischio di smarrimento e di furto è da considerarsi elevatissimo.

X. VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o di perdita a causa di virus informatici, il Titolare del trattamento dei dati stabilisce quali protezioni *software* adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.
Il Titolare del trattamento dei dati stabilisce inoltre la periodicità, non superiore a sei mesi, con cui debbono essere effettuati gli aggiornamenti dei sistemi antivirus utilizzati per ottenere un accettabile standard di sicurezza delle banche dati trattate.

I criteri debbono essere definiti dal Titolare del trattamento in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. In particolare per ogni sistema debbono essere definite le seguenti specifiche:

- Il tipo di programma utilizzato;
- La periodicità degli aggiornamenti.

Nel caso in cui su uno o più sistemi si dovesse verificare la perdita di informazioni o danni a causa di infezione o contagio da virus informatici il Titolare del trattamento deve provvedere ad attivare tutti i sistemi di risanamento idonei al recupero dell'elaboratore infetto, all'impedimento della propagazione del virus ed alla protezione della rete da attacchi futuri analoghi.

XI. ALTRE MISURE DI SICUREZZA

Il DPR 318/1999 vieta a chiunque di:

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

Il Titolare del trattamento dei dati 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 responsabile, 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 del trattamento dei dati deve informare con una comunicazione scritta l'Incaricato dell'ufficio dei compiti che gli sono stati affidati (lettera di incarico) e deve provvedere a formarlo affinché le mansioni indicate nella lettera gli siano familiari.

ASSEGNAZIONE NOMI UTENTE

Il Titolare del trattamento dei dati deve definire le modalità di assegnazione dei nomi identificativi per consentire a ciascun Incaricato del 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 Incaricato del trattamento deve essere annullato se l'Incaricato del trattamento ha dato le dimissioni.

ASSEGNAZIONE DELLE PASSWORD

Il Titolare del trattamento dei dati deve definire le modalità di assegnazione delle *password* e decidere che ogni utente Incaricato del 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 del trattamento dei dati 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 del trattamento 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 del trattamento dei dati circa ogni variazione dell'elenco degli Incaricati del trattamento autorizzati al trattamento dei dati personali.
In particolare, in caso di trattamento automatizzato di dati, per ogni Incaricato del trattamento deve essere indicato lo USER ID assegnato.

In caso di dimissioni di un Incaricato del trattamento o di revoca delle autorizzazioni al trattamento dei dati, il Responsabile del trattamento dei dati deve darne immediata comunicazione al Custode delle *password* (se diverso dal Titolare) che provvederà a disattivare la possibilità di accesso al sistema per il soggetto in questione.
Al Titolare del Trattamento 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.
Al Titolare del Trattamento è affidato il compito di redigere e di aggiornare ad ogni variazione la Tabella dei permessi di accesso che indica per ogni banca di dati i tipi di permesso di accesso per ogni Incaricato del trattamento autorizzato.
In particolare, per ogni Incaricato del 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.

XII. MANUTENZIONE DELLE APPARECCHIATURE

Al Titolare del trattamento 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 del trattamento 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 del trattamento 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 del trattamento deve prendere gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

XIII. LA VALUTAZIONE DI IMPATTO (D.P.I.A. – DATA PROTECTION IMPACT ASSESSMENT)

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal Titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal Regolamento Generale sulla Protezione dei Dati, è necessario eseguire la valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (articolo 35 del Regolamento 2016/679), ossia nei seguenti casi:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10 del Regolamento (c.d. sensibili e giudiziari);
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Nel percorso di analisi, normalmente, al fine di fornire un approccio scientifico alla scelta se eseguire o meno la DPIA vengono presi in considerazione 9 criteri al fine di verificare se il trattamento svolto sia tale da soddisfare due o più criteri (condizione necessaria per eseguire la DPIA):

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso del nostro Istituto, a parere del Data Protection Officer, i criteri 4, 5 e 7 sono da intendersi soddisfatti e pertanto il Titolare del Trattamento, d'accordo con il Responsabile della Protezione dei Dati, optano per l'esecuzione di tale analisi.

Si è detto che il G.D.P.R. predilige l'approccio all'analisi basato sul concetto di "rischio".
Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità.
L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** (gravità) di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DI ACCADIMENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	Molto probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE (GRAVITA')	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è la seguente:

PROBABILITA'					
	5	10	15	20	25
	4	8	12	16	20
	3	6	9	12	15
	2	4	6	8	10
	1	2	3	4	5
	1	2	3	4	5
	CONSEGUENZE				

Entità Rischio	Valori di riferimento
ACCETTABILE	$(1 \leq LR \leq 3)$
MEDIO-BASSO	$(4 \leq LR \leq 6)$
RILEVANTE	$(8 \leq LR \leq 12)$
ALTO	$(15 \leq LR \leq 25)$

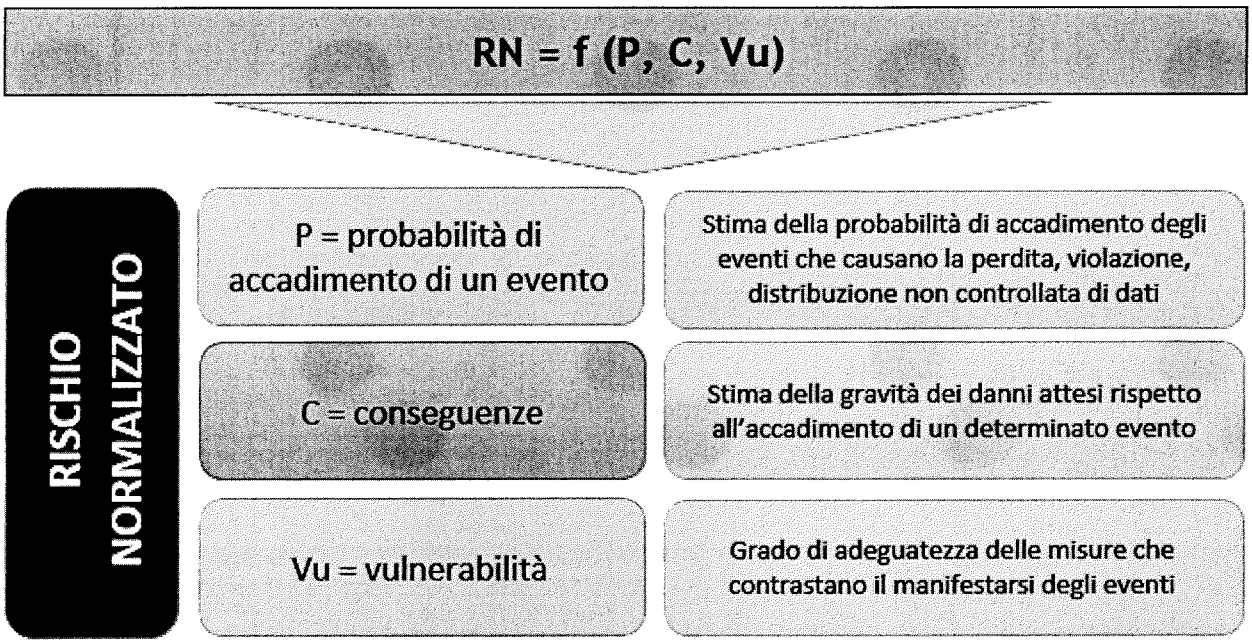
Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.

La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

RN = f (P, C, Vu)

RN = rischio normalizzato (sulla scuola)
P = probabilità
C = conseguenze generate dall'evento
V = Vulnerabilità rispetto al gradi di adeguatezza delle misure



In prima battuta viene ricavato il rischio intrinseco Ri come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori secondo il metodo ed i parametri già esposti alle pagine precedenti.

Esso viene ricavato prendendo in considerazione tutti i possibili pericoli e rischi basando la valutazione in funzione delle tipologie classiche di pericoli incombente sui dati e cioè:

Paragrafo XIV	Rischi riconducibili al cattivo comportamento degli operatori
Paragrafo XV	Rischi riconducibili al malfunzionamento delle apparecchiature
Paragrafo XVI	Rischi riconducibili ad eventi fisici ed atmosferici
Paragrafo XVII	Rischi specifici cui sono sottoposte le risorse connesse in rete internet

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla Vulnerabilità (Vu) è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA' (Vu)		
1	**Adeguate**	**0,25**
2	**Parzialmente adeguate**	**0,5**
3	**Inadeguate**	**1**

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori esposti in tabella.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

Vu	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	**Valori di riferimento**
MOLTO BASSO	$0,25 \leq RN \leq 1$
BASSO	$1 < RN < 3$
RILEVANTE	$3 \leq RN \leq 9$
ALTO	$12 \leq RN \leq 16$

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati che sono:

- AMMINISTRAZIONE DEGLI STUDENTI
- TRATTAMENTO GIURIDICO ED ECONOMICO DEL PERSONALE

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

ANALISI DEI RISCHI

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

XV. EVENTI DANNOSI IN SEGUITO A MALFUNZIONAMENTO DELLE APPARECCHIATURE

ANALISI DEI RISCHI

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

XVI. EVENTI DANNOSI IN SEGUITO AD EVENTI FISICI ED ATMOSFERICI

ANALISI DEI RISCHI

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

XVII. RISCHI SPECIFICI CUI SONO SOTTOPOSTE LE RISORSE CONNESSE AD INTERNET

ANALISI DEI RISCHI

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

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
Perdita - Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco (Ri)
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,25	Basso

PERICOLO		
Eventi naturali (terremoti, etc.)		
RISCHI		
Perdita - Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Gravi	Basso
VALUTAZIONE RISCHIO NORMALIZZATO		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Basso	0,5	Basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, etc.)		
RISCHI		
Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata – Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,5	Rilevante

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
Perdita + Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Limitate	Basso
VALUTAZIONE RISCHIO NORMALIZZATO		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Basso	0,5	Basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	0,5	Rilevante

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
Perdita - Distruzione non autorizzata - Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Rilevante	1	Rilevante

XVIII. 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

XIX. 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