ISTITUTO COMPRENSIVO FIGINO SERENZA

Via Europa, 25 22060 FIGINO SERENZA (CO)

DMTDP

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 G.D.P.R.)**
- **VALUTAZIONE D'IMPATTO (D.P.I.A.) (Art. 35 G.D.P.R.)**

Data di elaborazione del documento

11/03/2024

MODELLO REV. 1-2021

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

Redatto a cura e negli uffici di :
STUDIO AG.I.COM. S.R.L. UNIPERSONALE
Via XXV Aprile, 12 - 20070 SAN ZENONE AL LAMBRO (MI)
Tel. 02 90601324 Fax 02 700527180
R.E.A. - C.F. - P.IVA 05078440962
E-mail info@agicomstudio.it www.agicomstudio.it

SEDI IN CUI VENGONO TRATTATI I DATI (LUOGHI)

Al Titolare del trattamento è affidato il compito di vigilare sui trattamenti di dati personali svolti nell'ambito di ogni luogo a disposizione del Titolare stesso, affinchè venga svolto ad opera del solo personale a ciò autorizzato.

Per l'ente in oggetto i luoghi in cui avviene i trattamenti principali sono collocati presso:

ISTITUTO COMPRENSIVO FIGINO SERENZA
Via Europa, 25
22060 FIGINO SERENZA (CO)

Devono intendersi luoghi entro i quali avviene il trattamento dei dati anche i seguenti:

SCUOLA PRIMARIA "MARIA E MICHELE ORSENIGO" - Via Risorgimento, 8, Figino Serenza (CO)
SCUOLA PRIMARIA DI CARIMATE - Via Cesare Battisti, Carimate (CO)
SCUOLA PRIMARIA DI MONTESOLARO - Via Garibaldi, Montesolaro (CO)
SCUOLA PRIMARIA DI NOVEDRATE - Via per Mariano, Novedrate (CO)
SCUOLA SECONDARIA DI I GRADO DI CARIMATE - Via Aldo Moro, Carimate (CO)
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

ORGANIGRAMMA DEL TRATTAMENTO DEI DATI (PERSONE)

All'interno dell'Istituto il trattamento dei dati personali avviene ad opera di questi soggetti:

TITOLARE DEL TRATTAMENTO DEI DATI

L'ENTE NELLA PERSONA DEL RAPPRESENTANTE LEGALE

VINCENZO IAIA

AUTORIZZATI AL TRATTAMENTO

SOGGETTI INTERNI (DIPENDENTI E ASSIMILATI) CHE TRATTANO DATI IN NOME E PER CONTO DEL TITOLARE

ELENCO NOMINATIVO ALLE PAGINE CHE SEGUONO

RESPONSABILI DEL TRATTAMENTO

SOGGETTI ESTERNI CHE TRATTANO DATI IN NOME E PER CONTO DEL TITOLARE CON LORO ORGANIZZAZIONE AUTONOMA IN FORZA DI UN CONTRATTO

ELENCO NOMINATIVO ALLE PAGINE CHE SEGUONO

Il Titolare del trattamento ha individuato specialisti competenti che svolgono compiti di affiancamento tecnico-legale a garanzia dell'adozione di adeguate misure di sicurezza dei dati personali :

DATA PROTECTION OFFICER (D.P.O.)

LUCA CORBELLINI

INCARICATI TECNICI

(ordine alfabetico)

	COGNOME E NOME	SEDE / AZIENDA	RUOLO
1	ARGO SOFTWARE S.R.L.	Zona Industriale III Fase, 97100 Ragusa (RG)	AMM. DI PIATTAFORMA EST.
2	BRIGAGLIA SILVIA	SEDE	AMM. DI PIATTAFORMA INT.
3	CAIMI ANTONELLA	SEDE	AMM. DI PIATTAFORMA INT.
4	CAPPELLETTI CHIARA	SEDE	AMM. DI PIATTAFORMA INT.
5	COLANGELO SONIA	SEDE	AMM. DI PIATTAFORMA INT.
6	DUBINI MELISSA	SEDE	AMM. DI PIATTAFORMA INT.
7	FASOLI WILLIAM	I.I.S. "JEAN MONNET" MARIANO COMENSE	AMM. DI SISTEMA ESTERNO
8	FREGONESE NATIALIA	SEDE	AMM. DI PIATTAFORMA INT.
9	PAPPALARDO MADDALENA	SEDE	AMM. DI PIATTAFORMA INT.
10	POLLONI CLAUDIA	SEDE	AMM. DI PIATTAFORMA INT.
11	ZANFINO AGGEO	SEDE	ADD. MANUTENZ. INTERNO
12			
13			
14			
15			
16			
17			
18			
19			
20			

Alla pagina che segue il contenuto dei profili di autorizzazione per ciascun ruolo previsto per gli incaricati tecnici.

ELENCO NOMINATIVO DEGLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Ai fini del presente documento ed in ottemperanza a quanto previsto dal Regolamento UE 2016/679, con il termine "autorizzato" (o incaricato o designato) al trattamento dei dati personali, si intende il soggetto che esegue materialmente le operazioni di trattamento su tali dati con queste prerogative:

- Per tutto il tempo in cui svolgerà le predette mansioni nell'ambito di questo Titolare del trattamento;
- In modalità che potrà essere sia cartacea che digitale;
- Adottando, scrupolosamente, le misure di sicurezza espressamente riportate nel fascicolo recante "Istruzioni Operative", oggetto di formazione specifica somministrata a ciascun soggetto autorizzato.

AUTORIZZATO (ordine alfabetico)	**DESCRIZIONE SINTETICA DELLE AUTORIZZAZIONI**		
ALLEVI DANIELA	DOCENTE	VALUTAZIONE	SOMMINISTR. FARMACI
ARANTINO LIDIA	COLLABORATORE SCOLASTICO	SOMMINISTR. FARMACI	
ARNABOLDI RITA	DOCENTE	INCLUSIONE	SOMMINISTR. FARMACI
BELLOSI MARIA CRISTINA	DOCENTE	SOMMINISTR. FARMACI	
BIANCHI ANNAMARIA	DOCENTE	SOMMINISTR. FARMACI	
BONGIO MARIA LETIZIA	DOCENTE	CONTINUITA'	ORIENTAMENTO
BRIGAGLIA SILVIA	DOCENTE	REFERENTE DI PLESSO	VALUTAZIONE
BRIOSCHI DANIELE	DOCENTE	ALTRO	
BRUNO GIORDANO LUIGI	DOCENTE	PUBBLICAZIONE SITO	
BRUNO PAOLO	ASSISTENTE AMMIN.VO		
BUSILLO BARBARA	DOCENTE	SOMMINISTR. FARMACI	
CANNONE CAMILLA	DOCENTE	COLLABORATORE DEL D.S.	VALUTAZIONE
CAPETTI ANTONELLA	DOCENTE	PUBBLICAZIONE SITO	
CAPPELLETTI CHIARA	DOCENTE	PUBBLICAZIONE SITO	
CATTANEO ROSANGELA	DOCENTE	A.S.P.P. INTERNO	SOMMINISTR. FARMACI
CELENTANO IVANO	DOCENTE	ALTRO	
CERRETA LUCIA	DOCENTE	SOMMINISTR. FARMACI	
CHIAVELLA GRAZIELLA	REFERENTE DI PLESSO	R.L.S. INTERNO	VALUTAZIONE
CHIODO FILOMENA	DOCENTE	A.S.P.P. INTERNO	INCLUSIONE
CHIODO MITA GABRIELA	DOCENTE	SOMMINISTR. FARMACI	
COLOMBINI RENATA	DOCENTE	INCLUSIONE	ALTRO
COMOTTI LUCA	DOCENTE	PUBBLICAZIONE SITO	VALUTAZIONE
COSCIA GERARDINA	DOCENTE	CONTINUITA'	ORIENTAMENTO
COZZA MARIA LAURA	DOCENTE	VALUTAZIONE	
CROCI RITA	ASSISTENTE AMMIN.VO		
CROTTI MARIA GRAZIA	DOCENTE	REFERENTE DI PLESSO	VALUTAZIONE
DUBINI MELISSA	DOCENTE	ANIMATORE DIGITALE	INCLUSIONE
EPIFANIO EMANUELA	COLLABORATORE SCOLASTICO	SOMMINISTR. FARMACI	
FERRARA GIUSEPPINA	DOCENTE	CONTINUITA'	ORIENTAMENTO
FGRIGERIO VALERIA	DOCENTE	ALTRO	
FRAGONESE NATALIA	DOCENTE	PUBBLICAZIONE SITO	SOMMINISTR. FARMACI
FU PASQUALE MONTEFALCHESI LAURA	DOCENTE	SOMMINISTR. FARMACI	
GALESSI CHIARA	DOCENTE	CONTINUITA'	ORIENTAMENTO
GRAZIANO ROSA MARIA	DOCENTE	CONTINUITA'	ORIENTAMENTO
LA BRACA IVANA	DOCENTE	INCLUSIONE	INTERCULTURA

ELENCO NOMINATIVO DEGLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI (segue)

AUTORIZZATO (ordine alfabetico)	**DESCRIZIONE SINTETICA DELLE AUTORIZZAZIONI**		
LAZZARO TIZIANA	DOCENTE	A.S.P.P. INTERNO	SOMMINISTR. FARMACI
LEVERA MARCO	DOCENTE	REFERENTE DI PLESSO	VALUTAZIONE
LONGATTI ANNA	DOCENTE	VALUTAZIONE	
MALETTA ROSALBA	DOCENTE	A.S.P.P. INTERNO	ALTRO
MANDATO ANTONIETTA	COLLABORATORE SCOLASTICO	SOMMINISTR. FARMACI	
MARELLI LISA	DOCENTE	REFERENTE DI PLESSO	VALUTAZIONE
MARZORATI ILEANA	DOCENTE	SOMMINISTR. FARMACI	
MOLTENI ALICE	DOCENTE	PUBBLICAZIONE SITO	
MORANDIN MARIASSUNTA	COLLABORATORE SCOLASTICO	SOMMINISTR. FARMACI	
MOSCATELLI ELENA	ASSISTENTE AMMIN.VO		
MOSCATELLI SILVIA	D.S.G.A.		
MOTTA CRISTINA	ASSISTENTE AMMIN.VO		
NOTARO DOMENICA	DOCENTE	VALUTAZIONE	SOMMINISTR. FARMACI
PAPPALARDO MADDALENA	VICARIO DEL D.S.	A.S.P.P. INTERNO	VALUTAZIONE
PAPPALARDO MADDALENA	DOCENTE	ALTRO	
PAVESI ANNA	INCLUSIONE	INTERCULTURA	ALTRO
PIGNATARO ANNA RITA	ASSISTENTE AMMIN.VO		
POLLONI CLAUDIA	DOCENTE	PUBBLICAZIONE SITO	
PORRO STEFANIA	DOCENTE	CONTINUITA'	ORIENTAMENTO
PUGLIESE GIUSEPPE	COLLABORATORE SCOLASTICO	SOMMINISTR. FARMACI	
ROMANO' RITA	DOCENTE	A.S.P.P. INTERNO	
SCUTERI PALMINA	DOCENTE	CONTINUITA'	ORIENTAMENTO
SIRACUSA MARIA LORENA	ASSISTENTE AMMIN.VO		
SORRENTINO ROSSELLA	DOCENTE	SOMMINISTR. FARMACI	
STILO MARIA	DOCENTE	SOMMINISTR. FARMACI	
TAURINO ADRIANA LUANA	DOCENTE	SOMMINISTR. FARMACI	
TOCCACVELI ROMINA	DOCENTE	VALUTAZIONE	
VISCONTI NADIA	DOCENTE	SOMMINISTR. FARMACI	
VOTANO ANGELA	DOCENTE	VALUTAZIONE	
ZANFINO AGGEO	ASSISTENTE TECNICO		

Il personale autorizzato, sopra elencato, esegue trattamenti secondo questi profili:

	CATEGORIE DI INTERESSATI E FINALITA'
D.S.G.A.	ALLIEVI ISCRITTI E LICENZIATI/DIPLOMATI PER FINALITA' GESTIONALI ED AMMINISTRATIVE PERSONALE ASPIRANTE, IN SERVIZIO, TRASFERITO ED IN QUIESCENZA PER FINALITA' CONNESSE AL LORO TRATTAMENTO ECONOMICO E GIURIDICO E PER IL LORO COORDINAMENTO (A.T.A.) FORNITORI PER FINALITA' DI NATURA CONTABILE E PER LA LORO SELEZIONE
ASSISTENTE AMMINISTRATIVO	ALLIEVI ISCRITTI E LICENZIATI/DIPLOMATI PER FINALITA' GESTIONALI ED AMMINISTRATIVE PERSONALE ASPIRANTE, IN SERVIZIO, TRASFERITO ED IN QUIESCENZA PER FINALITA' CONNESSE AL LORO TRATTAMENTO ECONOMICO E GIURIDICO FORNITORI PER FINALITA' DI NATURA CONTABILE E PER LA LORO SELEZIONE I TRATTAMENTI POSSONO ESSERE PARZIALI IN FUNZIONE DEL PIANO DI LAVORO COMUNICATO DAL D.S.G.A.
COLLABORATORE VICARIO DEL DIRIGENTE COLLABORATORE DEL DIRIGENTE	ALLIEVI ISCRITTI E LICENZIATI/DIPLOMATI PER FINALITA' GESTIONALI ED AMMINISTRATIVE PERSONALE ASPIRANTE, IN SERVIZIO, TRASFERITO ED IN QUIESCENZA PER FINALITA' CONNESSE AL LORO TRATTAMENTO ECONOMICO E GIURIDICO E PER IL LORO COORDINAMENTO FORNITORI PER FINALITA' DI NATURA CONTABILE E PER LA LORO SELEZIONE SVOLGE COMPITI DI COMPLETA SOSTITUZIONE DEL DIRIGENTE SCOLASTICO IN SUA ASSENZA
FUNZIONE STRUMENTALE PER L'INCLUSIONE	IL DOCENTE, IN AGGIUNTA ALLE AUTORIZZAZIONI AL TRATTAMENTO INERENTI AL PROPRIO RUOLO ORDINARIO, TRATTA DATI DI NATURA PARTICOLARE INERENTI ANCHE A SOGGETTI CON DISABILITA' O ALTRO BISOGNO SPECIFICO ANCHE SE NON APPARTENENTI ALLE CLASSI ASSEGNATE
FUNZIONE STRUMENTALE PER L'ORIENTAMENTO FUNZIONE STRUMENTALE PER LA CONTINUITA' FUNZIONE STRUMENTALE INVALSI FUNZIONE STRUMENTALE P.C.T.O. E ALTERNANZA FUNZIONE STRUMENTALE PER L'INTERCULTURA	IN AGGIUNTA ALLE AUTORIZZAZIONI AL TRATTAMENTO INERENTI AL PROPRIO RUOLO ORDINARIO, TRATTA, PER LA FINALITA' CONNESSA ALLA PROPRIA FUNZIONE E DEFINITA CHIARAMENTE IN SEDE DI DESIGNAZIONE, DATI INERENTI ANCHE A SOGGETTI NON APPARTENENTI ALLE PROPRIE CLASSI
MEMBRO DEL G.L.O.	IL DOCENTE, IN AGGIUNTA ALLE AUTORIZZAZIONI AL TRATTAMENTO INERENTI AL PROPRIO RUOLO ORDINARIO, TRATTA DATI DI NATURA PARTICOLARE INERENTI AI SOGGETTI CON DISABILITA' A FAVORE DEI QUALI E' STATO ISTITUITO IL G.L.O. DI CUI E' MEMBRO FORMALMENTE DESIGNATO DAL DIRIGENTE SCOLASTICO.
ANIMATORE DIGITALE FUNZIONE STRUMENTALE PER L'INNOVAZIONE	L'ANIMATORE DIGITALE TRATTA DATI DI NATURA PREVALENTEMENTE COMUNE IN AFFIANCAMENTO A DIRIGENTE E D.S.G.A. NELLA PROGETTAZIONE E REALIZZAZIONE DEI PROGETTI DI INNOVAZIONE DIGITALE CONTENUTI NEL PIANO NAZIONALE SCUOLA DIGITALE. IL TRATTAMENTO DATI DEVE INTENDERSI SOLO EVENTUALE E SPECIFICAMENTE RISERVATO ALLA FASE ESECUTIVA.

Segue dalla pagina precedente

RESPONSABILE ALLA PUBBLICAZIONE SUL SITO	IL SOGGETTO TRATTA I DATI AL FINE DI ATTUARE GLI OBBLIGHI DI PUBBLICITA' PREVISTI DALLA VIGENTE NORMATIVA NONCHE' LE PUBBLICAZIONI PER LE QUALI SI E' PREVENTIVAMENTE ACQUISITO ESPLICITO CONSENSO DEGLI INTERESSATI
ADDETTO ALLA SOMMINISTRAZIONE DI FARMACI	ALLIEVI FREQUENTANTI CHE ABBIANO RICHIESTO LA SOMMINISTRAZIONE DI FARMACI IN ORARIO SCOLASTICO E PER I QUALI L'ADDETTO ABBIA FORNITO LA PROPRIA DISPONIBILITA', LIMITATAMENTE ALLE INFORMAZIONI STRETTAMENTE NECESSARIE PER ESEGUIRE TECNICAMENTE TALE SOMMINISTRAZIONE
MEMBRO DELLA COMMISSIONE FORMAZIONE CLASSI	ALLIEVI ISCRITTI AL PRIMO ANNO DEL CICLO DI STUDI PER I QUALI SIA NECESSARIO AVERE UN INQUADRAMENTO GENERALE IN ORDINE AL LORO ANDAMENTO SCOLASTICO ED AI LORO BISOGNI EDUCATIVI SPECIFICI AL FINE DI COSTITUIRE GRUPPI CLASSE UNIFORMI
MEMBRO DEL COMITATO DI VALUTAZIONE	DOCENTI NEOASSUNTI O IN PASSAGGIO DI RUOLO PER I QUALI SIA NECESSARIO RICONOSCERE L'ADEGUATEZZA DELLE COMPETENZE PROFESSIONALI IN SEGUITO AD UNA VALUTAZIONE DELLE ATTIVITA' FORMATIVE PREDISPOSTE, DELLE ESPERIENZE DI INSEGNAMENTO E PARTECIPAZIONE ALLA VITA DELLA SCUOLA
TIROCINANTE / STAGISTA	I TRATTAMENTI DATI AVVENGONO IN SEGUITO ALL'AFFIANCAMENTO DI PERSONALE SCOLASTICO AL FINE DI FORNIRE ALL'AUTORIZZATO LE ABILITA' INDISPENSABILI AD ORGANIZZARE / PROGETTARE / REALIZZARE IN MODO COMPETENTE LE ATTIVITA' TIPICHE DEL RUOLO AFFIANCATO. IL TRATTAMENTO DEI DATI AVVIENE SOTTO STRETTA SORVEGLIANZA DEL SOGGETTO AFFIANCATO. I DATI TRATTATI NON POSSONO ESSERE DIVULGATI.
R.S.P.P. INTERNO A.S.P.P. REFERENTE PER LA SICUREZZA R.L.S.	IL SOGGETTO AUTORIZZATO, IN AGGIUNTA ALLE AUTORIZZAZIONI AL TRATTAMENTO INERENTI AL PROPRIO RUOLO ORDINARIO, TRATTA DATI DI NATURA PARTICOLARE E POTENZIALMENTE ANCHE DATI INERENTI ALLO STATO DI SALUTE (AD ESEMPIO IN SEGUITO AD INFORTUNI O PER L'ADEGUAMENTO DEI PIANI DI EMERGENZA), VOLTI AL CORRETTO SVOLGIMENTO DELL'INCARICO, LIMITATAMENTE AI LUOGHI DI LAVORO ASSEGNATI.
DOCENTE	IL DOCENTE ACCEDE A DATI DI NATURA IDENTIFICATIVA E DI ANDAMENTO SCOLASTICO DI TUTTI GLI ALLIEVI DELLE CLASSI ASSEGNATE, SIA STABILMENTE CHE PERIODICAMENTE (SUPPLENZE). ACCEDE INOLTRE, POTENZIALMENTE, A DATI DI NATURA PARTICOLARE (SALUTE) E GIUDIZIARIA, NEL CASO DI ALLIEVI CON BISOGNI EDUCATIVI SPECIALI, SEMPRE LIMITATAMENTE AI COMPONENTI DELLE CLASSI ASSEGNATE.
COLLABORATORE SCOLASTICO	IL COLLABORATORE SCOLASTICO, NELL'AMBITO DELLE PROPRIE MANSIONI DI ACCOGLIENZA E SORVEGLIANZA DEGLI ALLIEVI E DI LORO VIGILANZA ED ASSISTENZA NEI MODI E NEI TEMPI PREVISTI DAL CONTRATTO COLLETTIVO DI RIFERIMENTO, PUO' ACCEDERE AI LORO DATI IDENTIFICATIVI. ACCEDE AI DATI IDENTIFICATIVI DEL PERSONALE SCOLASTICO PER FINALITA' ORGANIZZATIVE IN AFFIANCAMENTO ALLA SEGRETERIA.

Segue dalla pagina precedente

ASSISTENTE TECNICO	L'ASSISTENTE TECNICO, NELL'AMBITO DELLE PROPRIE MANSIONI DI SUPPORTO TECNICO DIRETTO ALLA ATTIVITA' DIDATTICA LABORATORIALE, PUO' TROVARSI AD ACCEDERE AI DATI IDENTIFICATIVI DEGLI ALLIEVI E DEL PERSONALE (ORARIO DI SERVIZIO DEI DOCENTI ETC.).
PSICOLOGO / PSICOPEDAGOGISTA INTERNO	TRATTA I DATI RELATIVI A COLORO CHE RICHIEDONO L'ACCESSO ALLO SPORTELLO PSICOLOGICO ISTITUITO A SCUOLA AL FINE DI COSTRUIRE BUONE RELAZIONI ED UNA STABILE BASE DI CRESCITA SIA RIVOLTA AGLI ALLIEVI CHE AL PERSONALE CHE NE FACCIA RICHIESTA. SVOLGE ATTIVITA' DI CONSULENZA E SUPPORTO.

Tutti i soggetti autorizzati sopra elencati, hanno ricevuto una lettera di autorizzazione allo scopo di chiarire il perimetro di tali autorizzazioni.
Ogni autorizzato al trattamento riceve, oltre ad una formazione specifica organizzata a cadenza periodica, al fine di coprire anche i nuovi arrivati in corso di anno, anche un documento recante "Istruzioni operative" nel quale sono riportate le indicazioni specifiche a cui rifarsi durante le operazioni di trattamento dati.

ELENCO NOMINATIVO DEI RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

L'Art. 28 del G.D.P.R. prevede che il Titolare possa nominare un Responsabile che effettui il trattamento per suo conto.
Ai fini del presente documento ed in ottemperanza a quanto previsto dal Regolamento UE 2016/679, con il termine "Responsabile del trattamento dei dati personali", intendiamo un soggetto esterno (questa tendenza ad escludere che il Responsabile possa essere un dipendente del Titolare è di gran lunga l'interpretazione più convincente) che si occupa di trattare i dati in nome e per conto del Titolare.
Appurato che il Responsabile è un esterno, la conseguenza è che il Titolare non può esercitare, su di esso, quei poteri di indirizzo e controllo tipici del rapporto di lavoro subordinato, ed è proprio con il "Contratto di nomina a Responsabile del trattamento" che ciò avviene in seguito all'instaurazione di questo nuovo rapporto contrattuale.
Il contratto di nomina a Responsabile del trattamento quasi sempre affianca un "contratto sottostante" con il quale il Titolare ha individuato il soggetto esterno per svolgere un incarico che comporterà il trattamento di dati (R.S.P.P., Medico Competente, D.P.O., Tesoreria, Registro elettronico etc.), obiettivo di questo atto è proprio quello di integrare tale contratto sottostante per tutte quelle questioni che non sono disciplinate all'interno di questo (data breach, audit etc.).

	Studio AG.I.COM. S.r.l.	Via XXV Aprile, 12
	C/A Dott. Luca Corbellini	20070 SAN ZENONE AL LAMBRO (MI)
1	**LA DESIGNAZIONE DI PERSONALE INCARICATO DAL FORNITORE A DATA PROTECTION OFFICER (D.P.O.) DELL'ISTITUTO SCOLASTICO**	

	Cancelli Arch. Fabio & C. S.n.c.	Via Massimo d'Azeglio, 3
	C/A Arch. Fabio Cancelli	22069 CANTU' (CO)
2	**LA DESIGNAZIONE DI PERSONALE INCARICATO DAL FORNITORE A RESPONSABILE DEL SERVIZIO DI PREVENZIONE E PROTEZIONE (R.S.P.P.) DELL'ISTITUTO SCOLASTICO**	

	Cassa Rurale e Artigiana di Cantù	Corso Unità d'Italia, 11
	C/A Amministrazione	22063 CANTU' (CO)
3	**SERVIZIO DI CASSA**	

	Argo Software S.R.L.	Zona Industriale III Fase
	C/A Amministrazione	97100 RAGUSA (RG)
4	**LA FORNITURA DEL SERVIZIO DI GESTIONE DIGITALE DEGLI UFFICI DI SEGRETERIA**	

	Argo Software S.R.L.	Zona Industriale III Fase
	C/A Amministrazione	97100 RAGUSA (RG)
5	**LA FORNITURA DEL SERVIZIO DI GESTIONE DEL REGISTRO ELETTRONICO**	

ELENCO NOMINATIVO DEI RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

	Google ireland Limited	Gordon House, Barrow Street
	C/A Amministrazione	Dublin 4 Ireland
6	**LA FORNITURA DEL SERVIZIO DI PIATTAFORMA DIDATTICA DIGITALE**	

7		

8		

9		

10		

11		

12		

Il personale tecnico autorizzato esegue questa tipologia di trattamenti:

AMMINISTRATORE DI SISTEMA

BASE DATI E LORO TIPOLOGIA	CATEGORIE DI INTERESSATI E FINALITA'
DATI PERSONALI DI TUTTE LE TIPOLOGIE (COMUNI, PARTICOLARI E GIUDIZIARI)	DATI DI ALLIEVI, PERSONALE E FORNITORI, TRATTATI ALL'UNICO FINE DI GESTIONE E MANUTENZIONE DEGLI IMPIANTI DI ELABORAZIONE ENTRO CUI SONO CUSTODITI O DI LORO COMPONENTI SIA HARDWARE CHE SOFTWARE LIMITATAMENTE ALL'AMBITO / PIATTAFORMA DI COMPETENZA.

Quando interno all'Istituto Scolastico agisce in qualità di "AUTORIZZATO ALL'ACCESSO AL SISTEMA INFORMATICO" mentre, quando esterno, viene designato quale "RESPONSABILE DEL TRATTAMENTO" ai sensi dell'Art. 28 del G.D.P.R..

Di seguito i compiti assegnati:

Adottare sistemi di registrazione degli accessi (log) degli amministratori ai sistemi di elaborazione ed agli archivi. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo (almeno sei mesi);

Sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, antivirus, filtri etc.);

Monitorare lo stato dei sistemi, con particolare attenzione alla loro sicurezza;

Effettuare in prima persona o sovraintendere agli interventi di manutenzione hardware ed a quelli software su sistemi operativi e applicativi;

Sovrintendere all'operato di eventuali tecnici esterni;

Fare in modo che sia prevista la disattivazione dei codici identificativi personali (user-id), in caso di perdita della qualità che consentiva all'autorizzato l'accesso a PC, device e piattaforme, oppure nel caso di mancato utilizzo del codice per oltre sei mesi;

Gestire le password di root o di amministratore di sistema;

Collaborare con il Titolare del trattamento, i Responsabili ed il Data Protection Officer;

Informare senza ritardo il Titolare del trattamento di tutte le questioni che possano far temere il prodursi di un data breach e fornire assistenza allo stesso in ordine alla sua eventuale notifica al Garante ed agli interessati;

Adottare le misure di sicurezza previste dalla legge e dalle D.P.I.A. eseguite, all'infrastruttura informatica di competenza;

Redigere annualmente un resoconto in ordine alla rispondenza della infrastruttura informatica di competenza, ai requisiti di sicurezza previsti dalle normative vigenti;

Il personale tecnico autorizzato esegue questa tipologia di trattamenti:

ADDETTO ALLA GESTIONE/MANUTENZIONE DI SISTEMA INFORMATICO

BASE DATI E LORO TIPOLOGIA	CATEGORIE DI INTERESSATI E FINALITA'
DATI PERSONALI DI TUTTE LE TIPOLOGIE (COMUNI, PARTICOLARI E GIUDIZIARI)	DATI DI ALLIEVI, PERSONALE E FORNITORI, TRATTATI ALL'UNICO FINE DI GESTIONE E MANUTENZIONE DEGLI IMPIANTI DI ELABORAZIONE ENTRO CUI SONO CUSTODITI O DI LORO COMPONENTI SIA HARDWARE CHE SOFTWARE LIMITATAMENTE ALL'AMBITO / PIATTAFORMA DI COMPETENZA.

Quando interno all'Istituto Scolastico agisce in qualità di "AUTORIZZATO ALL'ACCESSO AL SISTEMA INFORMATICO" mentre, quando esterno, viene designato quale "RESPONSABILE DEL TRATTAMENTO" ai sensi dell'Art. 28 del G.D.P.R..

Di seguito i compiti assegnati:

Effettuare interventi di manutenzione e recupero di dati, documenti e archivi;

Eseguire richieste di spostamento, ricollocazione, distruzione di dati o archivi;

Acquisire e conservare temporaneamente i dati di log di accesso ad internet, quelli relativi ad attacchi di maleware in generale quali virus e trojan nonché quelli relativi a tentativi di intrusione;

Configurare periferiche di stampa ed acquisizione dati;

Configurare sistemi di backup del dati;

Allocare temporaneamente gli archivi dati su propri sistemi o cloud per consentire la regolare esecuzione degli interventi manutentivi o di configurazione;

In caso di ritiro di P.C. o device in genere e loro traslocazione temporanea presso laboratori tecnici per l'impossibilità di eseguire l'intervento in loco, adottare misure di sicurezza adeguate ad impedire a terzi l'accesso ai dati;

Eseguire interventi di pulizia dei sistemi da virus e di ottimizzazione delle prestazioni dei singoli device;

Installare software di gestione remota dei dati da attivare solamente previo informazione ed espresso consenso del soggetto a cui il PC / device è in uso;

Informare senza ritardo il Titolare del trattamento di tutte le questioni che possano far temere il prodursi di un data breach e fornire assistenza allo stesso in ordine alla sua eventuale notifica al Garante ed agli interessati;

-

Il personale tecnico autorizzato esegue questa tipologia di trattamenti:

AMMINISTRATORE DI PIATTAFORMA DIGITALE

BASE DATI E LORO TIPOLOGIA	CATEGORIE DI INTERESSATI E FINALITA'
DATI PERSONALI COMUNI	DATI DI ALLIEVI E PERSONALE, TRATTATI AL FINE DELLA CREAZIONE DELLE UTENZE DI ACCESSO ALL'AMBITO / PIATTAFORMA DI COMPETENZA E DELLA SUA AMMINISTRAZIONE.

L'incarico di amministrazione viene svolto sulle principali piattaforme in uso all'interno dell'Istituto scolastico (segreteria digitale, registro elettronico, piattaforma didattica integrata etc.).

Quando interno all'Istituto Scolastico agisce in qualità di "AUTORIZZATO ALL'ACCESSO AL SISTEMA INFORMATICO" mentre, quando esterno, viene designato quale "RESPONSABILE DEL TRATTAMENTO" ai sensi dell'Art. 28 del G.D.P.R..

Di seguito i compiti assegnati:

Assicurare la custodia delle credenziali amministrative per la gestione dei sistemi di autenticazione e autorizzazione in uso e di prossima attivazione;

Creare e gestire gli utenti assegnando a ciascuno solamente i poteri di accesso che gli sono propri, ossia la possibilità di accesso ai soli dati riferiti alle classi di pertinenza;

Creare, se necessario, gruppi di utenti in base alle loro risorse utilizzabili;

Prestare assistenza nell'attivazione e configurazione di servizi legati alla piattaforma, nell'ottica della dematerializzazione e digitalizzazione dei documenti;

Informare senza ritardo il Titolare del trattamento di tutte le questioni che possano far temere il prodursi di un data breach e fornire assistenza allo stesso in ordine alla sua eventuale notifica al Garante ed agli interessati;

-

-

-

-

-

-

Terminiamo questa parte introduttiva di presentazione anagrafica delle sedi in cui avviene il trattamento e dell' organigramma dello stesso, per passare, alle pagine che seguono, ad analizzare nello specifico le attività di trattamento svolte.

INDICE

I° SEZIONE – ANAGRAFICA, FINALITA', NORMATIVA

I.	Scopo del documento	10
II.	Ambito di applicazione del documento	10
III.	Fonti del diritto	11
IV.	I Soggetti del trattamento dei dati	11
	Il Titolare del trattamento	11
	Il Responsabile del trattamento	11
	Gli Autorizzati al trattamento	12

II° SEZIONE – REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

V.	Registro principale delle attività di trattamento dell'Istituto Scolastico	12
	Tabella B – Registro delle attività di trattamento	16
	Registro T1 – Amministrazione degli studenti	
	Registro T1-A – Didattica Digitale Integrata	
	Registro T2 – Trattamento giuridico ed economico del personale	
	Registro T3 – Gestione fornitori di beni e servizi e degli specialisti esterni	
	Registro T4 – Videosorveglianza (compilato solo se presente)	
	Registro TS – Trattamenti speciali (compilato solo se presente)	
	Richiami al D.M. 305 del 07 Dicembre 2006 (SCHEDE DEI TRATTAMENTI)	17

III° SEZIONE – VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

VI.	Le misure di sicurezza globali	21
	Uso di internet da parte dei soggetti del trattamento	21
	Uso della posta elettronica da parte dei soggetti del trattamento	21
	Uso del fax da parte dei soggetti del trattamento	21
	Distruzione di documenti da parte dei soggetti del trattamento	22
	Gestione della posta cartacea da parte dei soggetti del trattamento	22
VII.	Misure di sicurezza contro il rischio di distruzione o perdita dei dati	22
	Procedura di esecuzione del Back-up	22
VIII.	Altre misure di sicurezza	23
	Assegnazione nomi utente	23
	Assegnazione delle password	23
	Sicurezza delle trasmissioni dati	24
	Personale autorizzato al trattamento	24
IX.	Manutenzione delle apparecchiature	24
X.	Il Data Breach	25
XI.	La tutela degli interessati (procedura)	32

IV° SEZIONE – VALUTAZIONI PROGRAMMATICHE

XII.	Formazione degli autorizzati	37
XIII.	Revisioni	37

I. SCOPO DEL DOCUMENTO

Scopo di questo documento è di delineare il quadro delle misure 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 in materia.

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 autorizzati al 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 europeo.

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 autorizzati 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 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 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 autorizzati al 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 autorizzato un Codice identificativo personale (USER ID) per l'utilizzazione dell'elaboratore, che deve essere individuale e non riutilizzabile;
- Autorizzare i singoli autorizzati al 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 dell'ente siano applicate all'interno ed eventualmente al di fuori dello stesso, 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.

AUTORIZZATI AL 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 individuare uno o più autorizzati del trattamento dei dati. Tale designazione è funzionale (ma non strettamente obbligatorio) che avvenga per iscritto e che dal documento di autorizzazione siano facilmente desumibili i compiti che gli sono affidati.
Gli autorizzati al 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 autorizzati deve essere assegnata una parola chiave e un codice identificativo personale, salvo che non siano in uso altri sistemi di identificazione individuale.
La nomina degli autorizzati al trattamento deve essere controfirmata dall'interessato per presa visione e copia della stessa deve essere conservata a cura del Titolare/Responsabile del trattamento per la sicurezza dei dati in luogo sicuro.
Agli autorizzati al trattamento il Titolare/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 autorizzati è a tempo indeterminato e decade per revoca, per dimissioni o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

V. REGISTRO PRINCIPALE DELLE ATTIVITA' DI TRATTAMENTO DI DATI PERSONALI DELL'ISTITUTO SCOLASTICO

Il registro delle attività di trattamento di questo paragrafo è la parte principale di questo documento e fornisce una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dei dati personali.
Esso ha lo scopo di dare consapevolezza e condivisione interna del processo di gestione del dato.

Il suo contenuto è prescritto dall'art. 30 del GDPR, queste le informazioni da includere:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- finalità del trattamento, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Al fine di descrivere le misure di sicurezza tecniche ed organizzative attuate dall'Istituto a tutela dei dati, occorre eseguire una valutazione preliminare dei rischi incombenti su questi. Infatti il GDPR predilige l'approccio c.d. "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".

Un rischio è quindi 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 ragionevolmente attese dal verificarsi di tale evento (C).
Dalla combinazione di queste grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

$$LR = P \times C$$

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze (gravità dei danni attesi)

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

PROBABILITA' DELL'EVENTO
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
1 Trascurabili
2 Marginali
3 Limitate
4 Gravi
5 Gravissime

La matrice che scaturisce dalla combinazione di probabilità e conseguenze è rappresentata in figura seguente:

Probabilità	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Si ricava così, per ogni attività di trattamento, un livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati) che convenzionalmente riteniamo possa assumere i seguenti valori:

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	$(15 \leq LR \leq 25)$

Per ciascun trattamento censito infine, è necessario valutare se debba essere prodotta la DPIA, acronimo di "*Data Protection Impact Assessment*", ossia 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, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una 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), livello di rischio che si presume sussistere quando ci troviamo in almeno una di queste circostanze:

1. Viene eseguita 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;

2. Avviene 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;

3. Avviene la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Nel percorso di analisi, al fine di determinare l'obbligatorietà o meno della DPIA, il "Gruppo Articolo 29" ha introdotto 9 criteri di criticità del trattamento, qualora un'attività di trattamento dati soddisfi due o più di questi, la valutazione d'impatto sulla protezione dei dati deve intendersi obbligatoria e deve essere riproposta con regolarità negli anni successivi. Questi i 9 criteri:

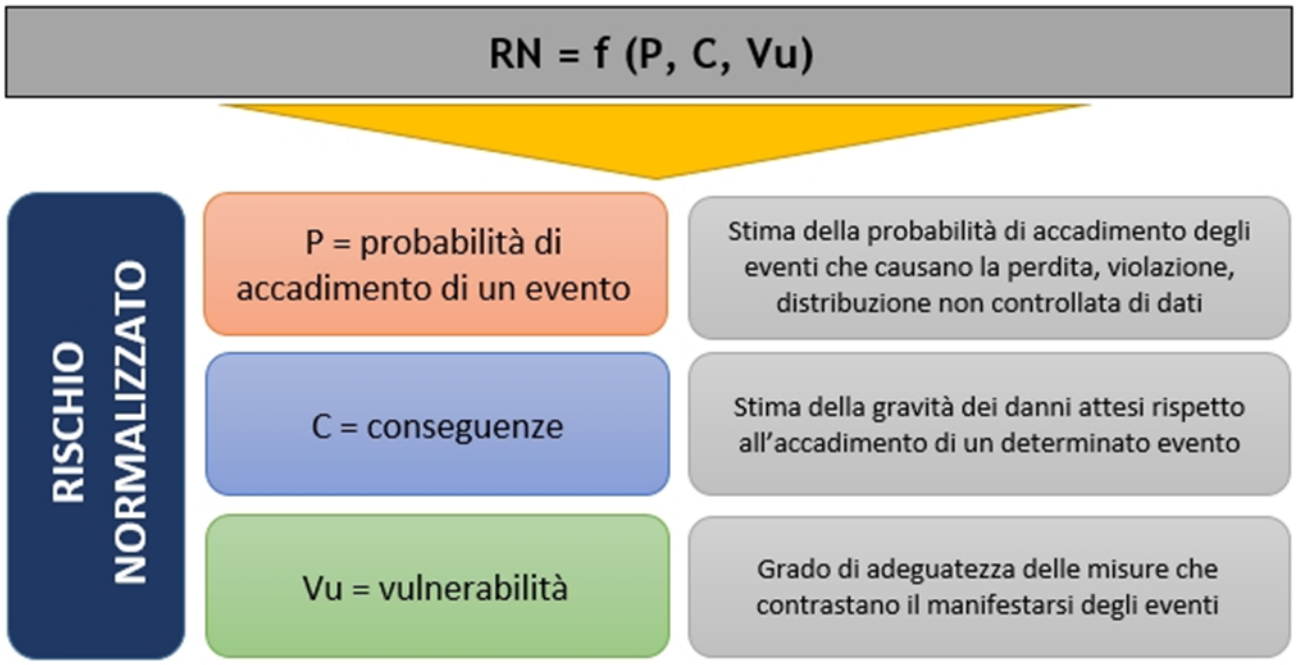
1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze 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

La DPIA, se necessaria, si basa su un'analisi dei rischi più dettagliata di quella di base descritta sopra, in cui si cerca di dare un peso ai possibili controlli applicabili, passando così da un indice di rischio "intrinseco" ad un indice di rischio "normalizzato" rispetto al contesto scolastico.

Il rischio (che definiamo "normalizzato") viene calcolato non più in funzione di 2 fattori, ma di 3:

$$RN = f\,(P, C, Vu)$$

P = probabilità
C = conseguenze generate dall'evento
Vu = vulnerabilità rispetto al grado di adeguatezza delle misure



Partendo dal valore di rischio (che chiamiamo convenzionalmente "Rischi Intrinseco") calcolato secondo la modalità prima descritta, 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'

1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

Quindi, 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 sopra indicati.

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	$12 \leq RN \leq 16$

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia ALTA, il Titolare attiva l'iter di consultazione del Garante.

Alle pagine che seguono sono elencati i trattamenti attivi relativi all'Istituto così identificato:

Titolare del trattamento dei dati	L'Istituto Scolastico intestatario del documento nella persona del rappresentante legale pro-tempore
Cotitolare del trattamento dei dati	Non presente
Data Protection Officer (D.P.O.)	Luca Corbellini c/o Studio AG.I.COM. S.r.l. unipersonale dpo@agicomstudio.it - agicom@pec.agicomstudio.it 02-90601324

Tabella B

Il registro principale è composto da più attività di trattamento:

Registro dell'attività T1	Trattamento dei dati degli allievi (Amministrazione degli studenti)
Sottoregistro T1-A	Didattica Digitale Integrata
Registro dell'attività T2	Trattamento economico e giuridico del personale
Registro dell'attività T3	Trattamento dei dati dei fornitori e degli specialisti esterni
Registro dell'attività T4	Trattamento delle immagini (Videosorveglianza se presente)
Registri speciali TS	Trattamenti specifici e temporanei (se presenti)

Che andiamo a rappresentare nel dettaglio alle pagine che seguono.

Registro T1	TRATTAMENTO DEI DATI DEGLI ALLIEVI (AMMINISTRAZIONE DEGLI STUDENTI)

Descrizione sommaria dell'attività di trattamento	Compete all'Istituto di Istruzione, la gestione amministrativa di tutti gli iscritti. Essa è fatta principalmente di attività c.d. "istituzionali" che trovano ragione nella diverse normative vigenti, ma anche di attività "libere", svolte per finalità di pubblico interesse e comunque riconducibili all'attività didattico-pedagogica principale, ma non espressamente previste dalle normative vigenti (la partecipazione ad un torneo, l'esposizione con pubblicazione dei risultati conseguiti, la pubblicazione a vario titolo di fotografie ed immagini etc.).	
Finalità del trattamento	ISCRIZIONE DEGLI ALLIEVI – ACQUISIZIONE E GESTIONE DELLE DOMANDE PRATICHE INERENTI AD ALLIEVI DIVERSAMENTE ABILI O CON PATOLOGIE DA GESTIRE IN ORARIO SCOLASTICO PARTECIPAZIONE DEI GENITORI/TUTORI ALLA ELEZIONE DEGLI ORGANI COLLEGIALI TENUTA DEI DATI INERENTI ALLA FREQUENZA SCOLASTICA ED AL RENDIMENTO DEGLI ALLIEVI GESTIONE DI DATI INERENTI ALL'ORIGINE ETNICA AL FINE DI FAVORIRE L'INTEGRAZIONE DEGLI STRANIERI GESTIONE DI DATI INERENTI ALLA FEDE RELIGIOSA AL FINE DI FAVORIRE L'INTEGRAZIONE DEGLI ALLIEVI GESTIONE DI DATI DI NATURA GIUDIZIARIA RIFERITI AD ALLIEVI E SOGGETTI ESERCENTI LA POTESTA SU DI QUESTI AL FINE DI FORNIRE SERVIZI INDIVIDUALIZZATI E SPECIFICI CERTIFICAZIONI ALLIEVI RISPETTO ALLA LORO FREQUENZA ED AI RISULTATI CONSEGUITI DENUNCE DI SINISTRI ED INFORTUNI DEGLI ALLIEVI PROCEDURE DI ORGANIZZAZIONE DEGLI ESAMI DI STATO TENUTA REGISTRO DIPLOMI RICHIESTE E TRASMISSIONE DI DOCUMENTI RICONDUCIBILI AGLI ALLIEVI RICONOSCIMENTO DI NULLAOSTA CORRISPONDENZA SCUOLA-GENITORI OSSERVATORIO OBBLIGO FORMATIVO GESTIONE DELLO SPORTELLO DIDATTICA APPLICAZIONE DELLE NORME DI IGIENE E SICUREZZA DEL LAVORO AGLI STUDENTI ASSIMILATI AI LAVORATORI AMMINISTRAZIONE DEGLI ALLIEVI STRANIERI (RILASCIO DI PERMESSI, VISTI DI RICONOSCIMENTI DI TITOLI) ADEMPIMENTI AGLI OBBLIGHI DI LEGGE CONSERVAZIONE SOSTITUTIVA DI TUTTI I DATI PIANIFICAZIONE DELLE ATTIVITÀ SELEZIONE E COSTITUZIONE DI GRADUATORIE A VARIO TITOLO	
Fonte dei dati	**Raccolti direttamente presso gli interessati**	
	LA QUASI TOTALITA' DEI DATI E' RACCOLTA DIRETTAMENTE PRESSO GLI INTERESSATI	
	Raccolti presso terzi	
	MINISTERO E UFFICI SCOLASTICI SUPERIORI RISPETTO A DATI DI NATURA ANAGRAFICA PER FINALITA' ORGANIZZATIVE COMUNE CON RIFERIMENTO AI DATI RELATIVI ALL'OBBLIGO DI FREQUENZA; COMUNE RISPETTO A SITUAZIONI SPECIFICHE FAMILIARI DA CONSIDERARE E GESTIRE; AZIENDA SANITARIA CON RIFERIMENTO AL PROFILO VACCINALE O EMERGENZE SANITARIWE IN CORSO FORZE DI POLIZIA E MAGISTRATURA PER LE QUESTIONI DI RILEVANZA PENALE O DI VOLONTARIA GIURISDIZIONE QUESTURA PER LE PRATICHE RELATIVE ALL'IMMIGRAZIONE	
Base giuridica	**Dati comuni (art. 6 GDPR)**	
	OBBLIGO SCOLASTICO (Legge 296/2006) CONTRATTO (ISCRIZIONE) CONSENSO (SOLO PER I TRATTAMENTI SVOLTI SU BASE VOLONTARIA E NON STRETTAMENTE ISTITUZIONALI)	
	Dati particolari (art. 9 GDPR)	
	OBBLIGO SCOLASTICO (Legge 296/2006) CONTRATTO (ISCRIZIONE) CONSENSO (SOLO PER I TRATTAMENTI SVOLTI SU BASE VOLONTARIA E NON STRETTAMENTE ISTITUZIONALI)	
Natura dei dati oggetto di trattamento	**Comuni**	**Termine trattamento**
	DATI ANAGRAFICI DELL'ALLIEVO E DEI SOGGETTI ESERCENTI LA POTESTA'; DATI ANAGRAFICI DEI SOGGETTI DELEGATI; DATI DI PRESENZA E DI RENDIMENTO SCOLASTICO.	ILLIMITATO PER FASCICOLI PERSONALI, REGISTRI DI ISCRIZIONE E PROVE DEGLI ESAMI DI STATO 50 ANNI PER I REGISTRI DEI VOTI E DELLE VALUTAZIONI E GLI SCRUTINI E I DATI RELATIVI ALLE BORSE DI STUDIO 6 ANNI PER GLI ELENCHI DEI LIBRI, LE CEDOLE E LE PRESENZE 1 ANNO PER GLI ELABORATI SCRITTI NON DI ESAME
	Particolari	**Termine trattamento**
	DATI DI NATURA SANITARIA RELATIVI ALLO STATO DI SALUTE DELL'ALLIEVO DISABILE O CHE ABBIA PATOLOGIE TALI DA PREVEDERE ATTIVITA' SPECIFICHE IN ORARIO SCOLASTICO; DATI DI NATURA SANITARIA RELATIVI ALLO STATO DI SALUTE DELL'ALLIEVO INFORTUNATO O CHE ABBIA PATITO UN SINISTRO; DATI IDONEI A RILEVARE LA FEDE RELIGIOSA DEGLI ALLIEVI E DEI SUOI FAMILIARI.	ILLIMITATO PER FASCICOLI PERSONALI
	Giudiziari	**Termine trattamento**
	DATI RELATIVI A CARICHI PENDENTI E PRECEDENTI PENALI DI ALLIEVI E SOGGETTI ESERCENTI LA POTESTA' SU DI QUESTI	ILLIMITATO PER FASCICOLI PERSONALI
Modalità di trattamento dati	I DATI VENGONO TRATTATI IN MODALITA' MISTA, SIA IN FORMATO CARTACEO CHE ELETTRONICO	
Categorie di	ALLIEVI	

interessati	SOGGETTI ESERCENTI LA POTESTA' SUGLI ALLIEVI SOGGETTI DELEGATI DAGLI ESERCENTI LA POTESTA' PER IL RITIRO O ALTRE PRATICHE			
Autorizzati al trattamento	**Interni**		**Trattamenti eseguiti**	
	PERSONALE DELLO STAFF DEL DIRIGENTE SCOLASTICO DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI PERSONALE AMMINISTRATIVO DELLA SEGRETERIA DIDATTICA DOCENTI DI CLASSE E DOCENTI DI SOSTEGNO ALLA CLASSE COLLABORATORI SCOLASTICI PERSONALE INCARICATO DI PRESTAZIONI DI ASSISTENZA INFORMATICA		RACCOLTA REGISTRAZIONE ORGANIZZAZIONE STRUTTURAZIONE CONSERVAZIONE CONSULTAZIONE ELABORAZIONE SELEZIONE ESTRAZIONE	RAFFRONTO UTILIZZO INTERCONNESSIONE BLOCCO COMUNICAZIONE DIFFUSIONE CANCELLAZIONE DISTRUZIONE
	Esterni (Responsabili del Trattamento)		**Trattamenti eseguiti**	
	PERSONALE INCARICATO DELL'ASSISTENZA INFORMATICA GESTORE DEL REGISTRO ELETTRONICO GESTORE DELLA PIATTAFORMA DI DIDATTICA A DISTANZA INCARICATO DEL RUOLO DI R.S.P.P. INCARICATO DEL RUOLO DI D.P.O. INCARICATO DEL RUOLO DI MEDICO COMPETENTE		REGISTRAZIONE ORGANIZZAZIONE STRUTTURAZIONE CONSERVAZIONE CONSULTAZIONE ELABORAZIONE SELEZIONE ESTRAZIONE	RAFFRONTO UTILIZZO INTERCONNESSIONE BLOCCO COMUNICAZIONE DIFFUSIONE CANCELLAZIONE DISTRUZIONE
Strutture entro le quali avviene il trattamento dati	**Dati in formato cartaceo**		**Archiviazione storica dati cartacei**	
	UFFICIO DEL DIRIGENTE SCOLASTICO E SUOI VICE SEGRETERIA DIDATTICA SALA DEI DOCENTI CASSETTI ED ARMADI NELLA DISPONIBILITA' DEI DOCENTI		ARCHIVIO DIDATTICO	
	Dati in formato elettronico		**Archiviazione storica dati elettronici**	
	SERVER DI SEGRETERIA CLOUD (REGISTRO ELETTRONICO) CLOUD (PIATTAFORMA DIDATTICA A DISTANZA)		UNITA' DI BACK UP DEL SERVER CONSERVATORIA DIGITALE (REGISTRO ELETTRONICO) CONSERVATORIA DIGITALE (PIATTAFORMA)	
	Software impiegati per il trattamento informatico dei dati in formato elettronico			
	SOFTWARE GESTIONALE D'ISTITUTO SOFTWARE GESTIONALE MINISTERIALE		REGISTRO ELETTRONICO PIATTAFORMA DIDATTICA A DISTANZA	
Possibili destinatari di attività di comunicazione	**Comunicazioni istituzionali**	**Extra UE**	**Comunicazioni su base volontaria**	**Extra UE**
	ENTI TERRITORIALI DELLO STATO AMMINISTRAZIONE SCOLASTICA I.N.A.I.L. AZIENDA SANITARIA LOCALE / A.T.S. R.S.P.P. D.P.O. MEDICO COMPETENTE ALTRI ISTITUTI SCOLASTICI	NO	AGENZIE VIAGGI COMPAGNIE DI ASSICURAZIONE SERVIZIO DI REFEZIONE (SE PREVISTO) FOTOGRAFI E VIDEOMAKER SITO INTERNET ISTITUZIONALE SOCIAL SCOLASTICI ALTRI ISTITUTI SCOLASTICI	NO
Informativa	VIENE FORNITA INFORMATIVA SPECIFICA CON RICHIESTA DI MANIFESTAZIONE DEL CONSENSO			
Profilazione	NON VIENE ATTUATA NESSUNA ATTIVITA' DI PROFILAZIONE			
Frequenza	IL TRATTAMENTO AVVIENE CON FREQUENZA QUOTIDIANA DURANTE IL PERIODO DI ATTIVITA' SCOLASTICA			
Valutazione del rischio	**TRATTAMENTO ANALIZZATO**	**PROBABILITA' (P)**	**CONSEGUENZE (C)**	**LIVELLO DI RISCHIO (LR)**
	ATTIVITA' GENERALE DELLA SEGRETERIA E DEGLI UFFICI	POCO PROBABILE [2]	GRAVI [4]	**RILEVANTE [8]**
	ATTIVITA' GENERALE DEI DOCENTI	POCO PROBABILE [2]	GRAVI [4]	**RILEVANTE [8]**
	ATTIVITA' DI SEGRETERIA CHE COMPORTANO IL RICORSO ALLA FIRMA GRAFOMETRICA E/O DIGITALE	IMPROBABILE [1]	GRAVI [4]	**MEDIO BASSO [4]**
	ATTIVITA' DI SEGRETERIA E DOCENTI SVOLTA MEDIANTE IL REGISTRO ELETTRONICO	POCO PROBABILE [2]	GRAVI [4]	**RILEVANTE [8]**
	ATTIVITA' DEI DOCENTI SVOLTA MEDIANTE PIATTAFORMA DIDATTICA A DISTANZA	POCO PROBABILE [2]	LIMITATE [3]	**MEDIO BASSO [6]**
Valutazione della obbligatorietà della DPIA	L'esito della valutazione dei rischi mostra un livello di rischio ELEVATO per i diritti e le libertà delle persone fisiche interessate ?			**NO**
	L'attività comporta procedimenti valutativi, di scoring o di profilazione ?			**NO**
	L'attività comporta la presa di decisioni automatizzate che producono significativi effetti giuridici (ammissioni, assunzioni, concessioni etc.) ?			**NO**
	L'attività comporta il monitoraggio sistematico di persone fisiche (videosorveglianza ad esempio) ?			**NO**
	L'attività comporta il trattamento di dati particolari, giudiziari o di natura estremamente personale (es. opinioni politiche) ?			**SI**
	L'attività comporta il trattamento di dati personali su larga scala ?			**NO**
	L'attività comporta la combinazione o il raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo			**NO**

	modalità che esulano dal contesto iniziale (big data) ?	
	L'attività comporta il trattamento di dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani etc.) ?	**SI**
	L'attività comporta utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (riconoscimento facciale ad esempio) ?	**NO**
	L'attività comporta trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).	**NO**
SI CONCLUDE LA VALUTAZIONE A FAVORE DELL'OBBLIGO DI ESEGUIRE LA DPIA PER QUESTO TRATTAMENTO		

	TRATTAMENTO	**RISCHIO INTRINSECO (Ri)**	**VULNERABILITA' (Vu)** SI CONSIDERA IL VALORE PEGGIORE	**RISCHIO NORMALIZZATO**
Valutazione del rischio su questo trattamento a valle della DPIA	ATTIVITA' GENERALE DELLA SEGRETERIA E DEGLI UFFICI	RILEVANTE [8]	PARZ. ADEGUATO [0,5]	**RILEVANTE [4]**
	ATTIVITA' GENERALE DEI DOCENTI	RILEVANTE [8]	ADEGUATO [0,25]	**BASSO [2]**
	ATTIVITA' DI SEGRETERIA CHE COMPORTANO IL RICORSO ALLA FIRMA GRAFOMETRICA E/O DIGITALE	MEDIO BASSO [4]	ADEGUATO [0,25]	**MOLTO BASSO [1]**
	ATTIVITA' DI SEGRETERIA E DOCENTI SVOLTA MEDIANTE IL REGISTRO ELETTRONICO	RILEVANTE [8]	ADEGUATO [0,25]	**BASSO [2]**

AL FINE DEL CONTENIMENTO DEL RISCHIO SONO ADOTTATE LE SEGUENTI MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE:

MISURA DI SICUREZZA	**RISCHIO CONTRASTATO**	**ADEGUATEZZA (Vu)**
E' adottata una politica di istituto per la sicurezza e la protezione dei dati ed all'interno dell'Istituto sono definiti i ruoli e le responsabilità di ciascuno anche mediante consegna di lettere di autorizzazione dettagliate	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni nella posta elettronica o nelle trasmissioni telematiche, etc.); - Azioni non autorizzate (errori volontari o involontari, introduzione di virus, uso non autorizzato di strumentazione elettronica quali chiavette USB, etc.).	ADEGUATO
Sono utilizzati software antivirus e firewall	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni nella posta elettronica o nelle trasmissioni telematiche, etc.); - Azioni non autorizzate (errori volontari o involontari, introduzione di virus, uso non autorizzato di strumentazione elettronica quali chiavette USB, etc.).	ADEGUATO
Vengono attuati i *back up* con frequenza quotidiana	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Interruzione servizi (sbalzi di tensione, guasti all'impianto, interruzione collegamenti di rete, etc.); - Furto di dati e distruzione volontaria ed involontaria.	ADEGUATO
Sono applicate, da parte del soggetto incaricato dell'amministrazione del sistema informatico, procedure di "*disaster recovery*" che garantiscono il ripristino dell'accesso ai dati in tempi ridotti	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Interruzione servizi (sbalzi di tensione, guasti all'impianto, interruzione collegamenti di rete, etc.); - Azioni di danneggiamento volontario.	PARZIALMENTE ADEGUATO DEVE ESSERE ESEGUITA FISICAMENTE UNA PROVA DI DISASTER RECOVERY ALL'ANNO
Sono adottati sistemi di cifratura e anonimizzazione dei dati relativi allo stato di salute delle persone	- Azioni non autorizzate (errori volontari o involontari, introduzione di virus, uso non autorizzato di strumentazione elettronica quali chiavette USB, etc.). - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni nella posta elettronica o nelle trasmissioni telematiche, etc.); - Furto e sottrazione di dati	PARZIALMENTE ADEGUATO OCCORRE ASSICURARE LA CIFRATURA DEL DISCO FISSO LOCALE O DI SUE PARTI (CARTELLE)
Sono registrati da parte del soggetto incaricato dell'amministrazione del sistema informatico, i "*log-file*" al fine di ricostruire gli accessi ai database	- Azioni non autorizzate (errori volontari o involontari, introduzione di virus, uso non autorizzato di strumentazione elettronica quali chiavette USB, etc.). - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni nella posta elettronica o nelle trasmissioni telematiche, etc.).	PARZIALMENTE ADEGUATO OCCORRE INSTALLARE IL SOFTWARE DI REGISTRAZIONE ONLINE DEI LOG
Viene eseguita periodica manutenzione della rete informatica in cui si esegue il trattamento dei dati al fine di controllare periodicamente il funzionamento regolare di antivirus, firewall nonché assicurare l'aggiornamento dei sistemi operativi in uso e di tutti i presidi di sicurezza attiva	- Problemi tecnici (anomalie e malfunzionamento software, problemi hardware).	ADEGUATO
I Data Center di cui l'Istituto di serve sono in possesso di certificazione ISO	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni nella posta elettronica o nelle trasmissioni telematiche, etc.); - Azioni non autorizzate (errori volontari o involontari, introduzione di virus, uso non autorizzato di strumentazione elettronica quali chiavette USB, etc.).	ADEGUATO

	- Problemi tecnici (anomalie e malfunzionamento software, problemi hardware).	
I singoli incaricati vengono formalmente autorizzati al trattamento dei dati ed a ciascuno vengono fornite credenziali personali (nome utente e *password*) per eseguire l'accesso ai sistemi informatici	- Azioni non autorizzate (errori volontari o involontari, introduzione di virus e malware in genere, uso non autorizzato di strumentazione elettronica quali chiavette USB, etc.). - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni nella posta elettronica o nelle trasmissioni telematiche, etc.); - Problemi tecnici (anomalie e malfunzionamento software).	ADEGUATO
Le credenziali di autenticazione fornite ai singoli incaricati sono disattivate in caso di assenza della persona prolungata per oltre 6 mesi	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni nella posta elettronica o nelle trasmissioni telematiche, etc.); - Azioni non autorizzate (errori volontari o involontari, uso non autorizzato di strumentazione, etc.).	ADEGUATO
Le credenziali di autenticazione fornite ai singoli incaricati sono disattivate o i profili di accesso sono modificati per colui che, a causa di un cambiamento di mansione, perda la possibilità di trattare i dati o se la veda modificata	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni nella posta elettronica o nelle trasmissioni telematiche, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	ADEGUATO
I sistemi di autorizzazione prevedono la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc. eseguita da parte di chi non è più autorizzato a trattare i dati).	ADEGUATO
Le parole chiave (*password*) fornite sono complesse (lunghe almeno 8 caratteri e formate da lettere e numeri, maiuscole e minuscole) e non sono riferibili a condizioni personali dell'autorizzato. Le password devono essere modificate la primo accesso e devono essere cambiate ogni 3 mesi	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Evitare che l'accesso ai dati digitali possa avvenire troppo facilmente.	ADEGUATO
Esclusivamente ai singoli incaricati viene concesso l'accesso ai locali (uffici, sale docenti, archivi, CED etc.) ed agli arredi (cassetti, armadi, schedari etc.) in cui devono prestare la loro attività di trattamento	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Evitare che l'accesso ai dati cartacei ed agli elaboratori possa avvenire troppo facilmente.	ADEGUATO
I locali in cui avviene il trattamento dati sono dotati di presidi antincendio	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.);	ADEGUATO
Le prese di alimentazione elettrica a cui sono connessi gli apparati informatici di rete nonché server ed elaboratori forniscono idonee garanzie di stabilità	- Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Interruzione servizi (sbalzi di tensione, guasti all'impianto, interruzione collegamenti di rete, etc.).	ADEGUATO
I locali in cui avviene il trattamento dati, al termine dell'attività, vengono chiusi a chiave così come cassetti ed armadi contenenti dati personali, le chiavi sono nella disponibilità di soli soggetti autorizzati a detenerle	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware).	ADEGUATO
I supporti cartacei contenenti dati personali non più necessari vengono distrutti fisicamente prima della loro eliminazione	- Accesso da parte di soggetti non autorizzati;	ADEGUATO
I supporti magnetici (chiavette, dischi removibili etc.) contenenti dati personali non più necessari vengono distrutti fisicamente prima della loro eliminazione	- Accesso da parte di soggetti non autorizzati;	ADEGUATO
Ai singoli utenti autorizzati vengono fornite istruzioni per la custodia e l'uso di supporti removibili	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Perdita, smarrimento, furto.	ADEGUATO
E' prevista l'organizzazione periodica di corsi di formazione ed interventi informativi volti a fornire nozioni ed a sensibilizzare il personale autorizzato	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Perdita, smarrimento.	ADEGUATO
Il personale autorizzato è soggetto alla vigilanza del Titolare del trattamento	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.);	ADEGUATO

e degli altri autorizzati con compiti di coordinamento e direttivi	- Furti, danneggiamenti volontari; - Uso non autorizzato di supporti personali; - Uso illegale di software.	
Tutte le procedure sono oggetto di riesame almeno annuale in occasione dell'audit periodico eseguito dal D.P.O.	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Verifica della corretta applicazione delle norme regolamentari.	ADEGUATO
I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	ADEGUATO
Sono definiti termini di conservazione e le condizioni di impiego e successiva distruzione dei dati personali trattati	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.).	ADEGUATO
Su questo trattamento viene eseguita la DPIA (Data Protection Impact Assesment)	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	ADEGUATO

Registro T1	**TRATTAMENTO DEI DATI DEGLI ALLIEVI (AMMINISTRAZIONE DEGLI STUDENTI)**
Sottoregistro A	**DIDATTICA DIGITALE INTEGRATA REALIZZATA CON GOOGLE WORKSTATION**

Descrizione sommaria dell'attività di trattamento	Dopo la pandemia la didattica eseguita mediante metodologie digitali si è affermata ed evoluta come metodo integrativo rispetto all'esperienza tradizionale dei nostri Istituti, giugnendo ad assumere un ruolo centrale al pari di quella tradizionalmente intesa. Essa viene progettata dal personale docente in modo da assicurare le medesime garanzie da sempre adottate per la formazione frontale: sostenibilità delle attività proposte e inclusività in primis, intendendo in senso ampio tale termine considerando anche aspetti come la facilità di connessione, la qualità della stessa, la presenza di device adeguati ed affidabili nonché la conoscenza degli stessi. Google Workspace è un pacchetto di applicazioni che consente di interagire secondo modalità collaborative anche a distanza, a beneficio della didattica. In particolare sono questi i servizi in uso: • **Google Classroom**: classe virtuale utile per comunicare, trasmettere materiali, compiti e rammentare scadenze in modalità online. • **Google Drive** spazio virtuale dove creare, archiviare, condividere e modificare documenti direttamente online, anche in modalità collaborativa e senza necessità che sul proprio computer sia installato alcun programma, semplicemente accedendo tramite il proprio account. • **Google Meet** per l'attività di teleconferenza (riunioni e lezioni). Per poter utilizzare queste applicazioni ad ogni docente e ad ogni allievo viene assegnata una casella di posta elettronica (Gmail) con un indirizzo composto da una parte personale (cognome e nome o altro codice) seguito dal nome del dominio di Istituto. Le credenziali consentono a chi dispone di una casella di consultare la posta altre ad accedere ai diversi servizi didattici.	
Finalità del trattamento	Le finalità perseguite dal trattamento in oggetto sono essenzialmente quelle della gestione della lezione online e della valutazione degli allievi oltre alla tenuta dei dati inerenti alla frequenza scolastica, al rendimento ed agli aspetti burocratici connessi alla gestione didattica dell'iscrizione a scuola, operata dal personale docente. L'Istituto promuove, nell'ambito del Piano Triennale dell'Offerta Formativa (P.T.O.F.) e in collaborazione con il Ministero, azioni coerenti con le finalità, i principi e gli strumenti previsti nel PNSD (L. 107/2015, art. 1, commi 56 e 57). Il Piano scolastico per la didattica digitale integrata è stato approvato dal Collegio Docenti.	
Fonte dei dati	**Raccolti direttamente presso gli interessati**	
	LA TOTALITA' DEI DATI E' RACCOLTA DIRETTAMENTE PRESSO GLI INTERESSATI	
	Raccolti presso terzi	
	NESSUNO	
Base giuridica	**Dati comuni (art. 6 GDPR)**	
	OBBLIGO SCOLASTICO (Legge 296/2006) CONTRATTO (ISCRIZIONE) Il trattamento dei dati personali da parte delle istituzioni scolastiche è necessario in quanto collegato all'esecuzione di un compito di interesse pubblico di cui è investita la scuola attraverso una modalità operativa prevista dalla normativa Il consenso dei genitori, che non costituisce una base giuridica idonea per il trattamento dei dati in ambito pubblico e nel contesto del rapporto di lavoro, non è richiesto perché l'attività svolta, sia pure in ambiente virtuale, rientra tra le attività istituzionalmente assegnate all'istituzione scolastica, ovvero di didattica nell'ambito degli ordinamenti scolastici vigenti. Pertanto, l'Istituto è legittimato a trattare tutti i dati personali necessari al perseguimento delle finalità collegate allo svolgimento della DDI nel rispetto dei principi previsti dalla normativa di settore. La Scuola ha redatto un proprio Piano per la Didattica Digitale Integrata e adottato un Regolamento approvato dal Collegio Docenti e dal Consiglio d'Istituto.	
	Dati particolari (art. 9 GDPR)	
	NESSUNO	
Natura dei dati oggetto di trattamento	**Comuni**	**Termine trattamento**
	INFORMAZIONI SUL DISPOSITIVO SISTEMA OPERATIVO IN USO RETE MOBILE IN USO INDIRIZZO IP INFORMAZIONI DI LOG INFORMAZIONI SULLA POSIZIONE (TRAMITE IP) VERSIONI DELLE APPLICAZIONI IN USO BROWSER IN USO SOFTWARE DI GESTIONE DELLA POSTA IN USO LINGUA PREFERITA DATI DI VARIA NATURA CONDIVISI TRAMITE GLI STRUMENTI IN USO (CLASSROOM, DRIVE, MEET, MAIL).	I DATI RELATIVI ALLA DIDATTICA DIGITALE INTEGRATA SARANNO CONSERVATI PRESSO IL FORNITORE PER TUTTA LA DURATA DI PERMANENZA DELL'ALLIEVO PRESSO L'ISTITUTO, DOPO DI CHE, AL TERMINE DELL'ULTIMO ANNO SCOLASTICO DI FREQUENZA, L'ISTITUTO ORDINERÀ AL FORNITORE LA DISTRUZIONE DEI DATI CHE AVVERRÀ ENTRO IL TERMINE TECNICO DI 180 (CENTOTTANTA) GIORNI. I DATI SCOLASTICI IN SENSO STRETTO (ELABORATI, REGISTRAZIONI VIDEO, ETC.) SARANNO CONSERVATI PER LA TEMPISTICA PREVISTA DALLA LEGGE (ESCLUSIVAMENTE PER LE PROVE VALUTATIVE, LA CIRCOLARE N° 44 DEL 19/12/2005 DELLA DIREZIONE GENERALE PER GLI ARCHIVI - "ARCHIVI DELLE ISTITUZIONI SCOLASTICHE" PRESCRIVE LA CONSERVAZIONE DI ELABORATI DELLE PROVE SCRITTE, GRAFICHE E PRATICHE PER ALMENO UN ANNO, E LA CONSERVAZIONE DI DOCUMENTAZIONE CAMPIONE UN ANNO OGNI DIECI)

		PER QUANTO CONCERNE IL PERSONALE DOCENTE I DATI SONO TENUTI ONLINE PER TUTTA LA DURATA DEL SERVIZIO (CONTRATTO DI LAVORO) IL MATERIALE DI VARIA NATURA CONDIVISO TRAMITE GLI STRUMENTI IN USO VIENE ARCHIVIATO DA PARTE DEI DOCENTI CHE SI BASERANNO ANCHE SU QUESTO PER LA LORO ATTIVITA' VALUTATIVA. TRATTANDOSI DI VERI E PROPRI ATTI AMMINISTRATIVI L'ARCHIVIAZIONE DOVRÀ ESSERE EFFETTUATA IN MODO TALE DA RENDERE NON ACCESSIBILE LA DOCUMENTAZIONE AGLI INTERESSATI, CHE POTRANNO AVERNE ACCESSO O RICHIEDERNE LA MODIFICA, RETTIFICA O CANCELLAZIONE SOLAMENTE TRAMITE RICHIESTA SCRITTA CHE NON LIMITI LE FINALITÀ ISTITUZIONALI DEL TRATTAMENTO, ORIENTATE AL CORRETTO SVOLGIMENTO DELL'ATTIVITÀ DIDATTICA.
	Particolari	**Termine trattamento**
	NESSUNO (E' IN USO UN DIVIETO DI COLLOCARE IN MODALITA' LEGGIBILE DATI DI NATURA PARTICOLARE SU DRIVE)	NESSUNO
	Giudiziari	**Termine trattamento**
	NESSUNO (E' IN USO UN DIVIETO DI COLLOCARE IN MODALITA' LEGGIBILE DATI DI NATURA GIUDIZIARIA SU DRIVE)	NESSUNO
Modalità di trattamento dati	I DATI VENGONO TRATTATI IN MODALITA' ELETTRONICA	
Categorie di interessati	ALLIEVI SOGGETTI ESERCENTI LA POTESTA' SUGLI ALLIEVI	
Autorizzati al trattamento	**Interni**	**Trattamenti eseguiti**
	DOCENTI DI CLASSE E DOCENTI DI SOSTEGNO ALLA CLASSE PERSONALE INCARICATO DI PRESTAZIONI DI ASSISTENZA INFORMATICA	RACCOLTA REGISTRAZIONE ORGANIZZAZIONE STRUTTURAZIONE CONSERVAZIONE CONSULTAZIONE ELABORAZIONE SELEZIONE ESTRAZIONE RAFFRONTO UTILIZZO INTERCONNESSIONE BLOCCO COMUNICAZIONE DIFFUSIONE CANCELLAZIONE DISTRUZIONE
	Esterni (Responsabili del Trattamento)	**Trattamenti eseguiti**
	PERSONALE INCARICATO DELL'ASSISTENZA INFORMATICA GESTORE DELLA PIATTAFORMA DI DIDATTICA A DISTANZA (GOOGLE)	REGISTRAZIONE ORGANIZZAZIONE STRUTTURAZIONE CONSERVAZIONE CONSULTAZIONE ELABORAZIONE SELEZIONE ESTRAZIONE RAFFRONTO UTILIZZO INTERCONNESSIONE BLOCCO COMUNICAZIONE DIFFUSIONE CANCELLAZIONE DISTRUZIONE
Strutture entro le quali avviene il trattamento dati	**Dati in formato cartaceo**	**Archiviazione storica dati cartacei**
	NESSUNO	NESSUNO
	Dati in formato elettronico	**Archiviazione storica dati elettronici**
	CLOUD (PIATTAFORMA DIDATTICA A DISTANZA)	CONSERVATORIA DIGITALE DI GOOGLE WORKSPACE
	Software impiegati per il trattamento informatico dei dati in formato elettronico	
	GOOGLE WORKSPACE	

Possibili destinatari di attività di comunicazione	**Comunicazioni istituzionali**	**Extra UE**	**Comunicazioni su base volontaria**	**Extra UE**
	AMMINISTRAZIONE SCOLASTICA	SI	NESSUNO	NO

Informativa	VIENE FORNITA INFORMATIVA SPECIFICA IN BASE ALLE DISPOSIZIONI CONTENUTE NEGLI ARTT. 13 E 14 DEL REGOLAMENTO UE 2016/679, L'ISTITUTO SI PREOCCUPA DI INFORMARE GLI INTERESSATI IN MERITO AI TRATTAMENTI DEI DATI PERSONALI EFFETTUATI NELL'AMBITO DELL'EROGAZIONE DELL'OFFERTA FORMATIVA. POICHÉ ATTRAVERSO L'UTILIZZO DELLA PIATTAFORMA PER L'EROGAZIONE DELLA DDI SONO TRATTATI SIA DATI DEGLI STUDENTI CHE DEI DOCENTI E, IN TALUNI CASI, ANCHE DEI GENITORI, LA SCUOLA FORNISCE A TUTTE QUESTE CATEGORIE DI INTERESSATI, DI REGOLA ALL'INIZIO DELL'ANNO SCOLASTICO, ANCHE NELL'AMBITO DI UNA SPECIFICA SEZIONE DELL'INFORMATIVA GENERALE O IN UN DOCUMENTO AUTONOMO, TUTTE LE INFORMAZIONI RELATIVE A TALI TRATTAMENTI.
Profilazione	NON VIENE ATTUATA NESSUNA ATTIVITA' DI PROFILAZIONE
Frequenza	IL TRATTAMENTO AVVIENE CON FREQUENZA QUOTIDIANA DURANTE IL PERIODO DI ATTIVITA' SCOLASTICA

Valutazione del rischio	**TRATTAMENTO ANALIZZATO**	**PROBABILITA' (P)**	**CONSEGUENZE (C)**	**LIVELLO DI RISCHIO (LR)**
	ATTIVITA' DEI DOCENTI SVOLTA MEDIANTE	POCO PROBABILE [2]	LIMITATE [3]	**MEDIO BASSO [6]**

	PIATTAFORMA DIDATTICA A DISTANZA			
Valutazione della obbligatorietà della DPIA	L'esito della valutazione dei rischi mostra un livello di rischio ELEVATO per i diritti e le libertà delle persone fisiche interessate ?			**NO**
	L'attività comporta procedimenti valutativi, di scoring o di profilazione ?			**NO**
	L'attività comporta la presa di decisioni automatizzate che producono significativi effetti giuridici (ammissioni, assunzioni, concessioni etc.) ?			**NO**
	L'attività comporta il monitoraggio sistematico di persone fisiche (videosorveglianza ad esempio) ?			**NO**
	L'attività comporta il trattamento di dati particolari, giudiziari o di natura estremamente personale (es. opinioni politiche) ?			**NO**
	L'attività comporta il trattamento di dati personali su larga scala ?			**NO**
	L'attività comporta la combinazione o il raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal contesto iniziale (big data) ?			**NO**
	L'attività comporta il trattamento di dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani etc.) ?			**SI**
	L'attività comporta utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (riconoscimento facciale ad esempio) ?			**NO**
	L'attività comporta trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).			**NO**
SI CONCLUDE LA VALUTAZIONE A FAVORE DELLA OPPORTUNITA' (NON OBBLIGO) DI ESEGUIRE LA DPIA PER QUESTO TRATTAMENTO				
Valutazione del rischio su questo trattamento a valle della DPIA	**TRATTAMENTO**	**RISCHIO INTRINSECO (Ri)**	**VULNERABILITA' (Vu)** SI CONSIDERA IL VALORE PEGGIORE	**RISCHIO NORMALIZZATO**
	ATTIVITA' DEI DOCENTI SVOLTA MEDIANTE GOOGLE WORKSPACE	MEDIO BASSO [6]	ADEGUATO [0,25]	**BASSO [1,5]**

AL FINE DEL CONTENIMENTO DEL RISCHIO SONO ADOTTATE LE SEGUENTI MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE:

MISURA DI SICUREZZA	RISCHIO CONTRASTATO	ADEGUATEZZA (Vu)
Il fornitore e' stato designato come responsabile del trattamento ?	Il contratto concluso con Google Ireland Ltd prevede che il fornitore acquisisca gli obblighi tipici del Responsabile del Trattamento dei dati come definito all'Art. 28 del GDPR. L'Istituto, in seguito alla Sentenza della Corte di Giustizia dell'Unione Europea del 16/07/2020, (c.d. Schrems II) ha verificato la adeguatezza degli strumenti proposti da Google a rendere il trattamento svolto conforme ai requisiti del GDPR in seguito all'adozione di misure tecniche e organizzative adeguate. Si dà atto inoltre che il software Google Workspace di Google Cloud Italy Srl risulta essere qualificato dal 27/11/2019 (rinnovato giunto lo scorso 19/01/2023) nella tipologia SaaS per la categoria: Servizi per la fiscalità, Servizi demografici, Servizi interni alle PA.	ADEGUATO
Il fornitore ha la propria sede all'interno dell'Unione Europea ?	Sì, la sede di Google Ireland Ltd si trova in Irlanda e conseguentemente la stessa è soggetto al Regolamento UE 679/2016, tuttavia l'architettura di Google Workspace conduce ad utilizzare infrastrutture site al di fuori della U.E. ed in particolare negli U.S.A., pertanto tale condizione non può essere considerata sufficiente a garantire la conformità del sistema. Questo fatto ha portato delle criticità in relazione alla sentenza C.311/18 con la quale la Corte di Giustizia ha dichiarato l'invalidità della decisione di adeguatezza Privacy Shield. Questa situazione si è risolta a far data dal 10/07/23 con il nuovo accordo transfrontaliero che prende il nome di "EU-US Data Privacy Framework" con il quale Bruxelles, ha formalmente riconosciuto che sussistono garanzie sufficienti per la protezione dei dati personali dei cittadini dell'UE trattati nel territorio statunitense, nonché tutele legali che insieme ai nuovi parametri sono in grado di limitare l'invasivo operato delle agenzie di intelligence USA. L l'Istituto adotta comunque delle misure precauzionali. In particolare, il personale scolastico tratta esclusivamente i dati strettamente necessari al perseguimento delle finalità didattiche e tramite i software di base, evitando il trattamento di dati particolari e giudiziari mediante Google Worskspace, quantomeno in modalità "in chiaro" (ossia adottando misure di crittografia estranee a quelle di Google).	ADEGUATO
Quali prodotti sono attivati ?	La suite dispone di diversi servizi integrati, alcuni sono da considerarsi "principali" ed indispensabili per la didattica mentre altri sono aggiuntivi e l'amministratore della piattaforma non deve attivarli salvo richiederne espresso consenso agli interessati. Sono in uso: Classroom, Drive, Meet e Mail.	ADEGUATO
Standard applicabili	L'European Data Protection Board (EDPD) ha pubblicato le "Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE", che specificano i comportamenti da seguire riguardo al trasferimento di dati all'estero.	ADEGUATO

	Il Ministero dell'Istruzione ha pubblicato nell'estate del 2020 le Linee Guida per la Didattica Digitale Integrata (DDI), previste dal Piano per la ripresa della scuola e passate al vaglio del Consiglio Superiore della Pubblica Istruzione. Il documento contiene indicazioni operative affinché ciascun Istituto scolastico possa dotarsi di un Piano scolastico per la didattica digitale integrata che dovrà essere allegato al Piano triennale per l'offerta formativa di ciascuna scuola. Dovranno essere coinvolte tutte le componenti della comunità scolastica fornendo apposita comunicazione a docenti, famiglie e studenti sui suoi contenuti. Ai sensi dalla circolare AGID n. 2 del 09/04/2018, le Pubbliche Amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati. In proposito Workspace di Google Cloud Italy Srl risulta essere qualificata dal 27/11/2019 nella tipologia SaaS per la categoria: Servizi per la fiscalità, Servizi demografici, Servizi interni alle PA. Si tenga presente anche quanto affermato dal Gruppo di lavoro congiunto Ministero dell'istruzioneUfficio del Garante per la protezione dei dati personali, di cui al Decreto del Capo di Gabinetto prot. n. 1885 del 5 giugno 2020, nel documento "Didattica Digitale Integrata e tutela della privacy: indicazioni generali" del settembre 2020 con il fine di fornire alle istituzioni scolastiche linee di indirizzo comuni e principi generali per l'implementazione della DDI con particolare riguardo agli aspetti inerenti alla sicurezza in rete e alla tutela dei dati personali. Si veda anche il Provvedimento del 26 marzo 2020 - "Didattica a distanza: prime indicazioni" del Garante per la Privacy. In ossequio a quanto affermato da Garante e Ministero quindi in piena pandemia non è stato necessario procedere alla valutazione di impatto, ex art. 35 del GDPR, considerato che l'Istituto non effettua trattamenti di dati personali su larga scala nell'ambito dell'utilizzo del servizio on line di videoconferenza (Google Meet) nè la piattaforma Google Workspace consente il monitoraggio sistematico degli utenti. Non si ricorre comunque a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici). L'Istituto ha provveduto comunque ad adottare documentazione (PDDI, regolamento, informative e guide) e le procedure volte a minimizzare i rischi per i dati personali dei soggetti interessati.	
Quali sono i dati acquisiti mediante uso della piattaforma ?	Oltre ai dati essenziali forniti dall'istituto all'atto della creazione delle utenze, l'utilizzo della piattaforma comporta l'acquisizione di informazioni aggiuntive quali: informazioni sul dispositivo (modello, sistema operativo, seriale e numero di telefono dell'utente). Informazioni di registro, attività svolte, informazioni sugli eventi del dispositivo e indirizzo del protocollo internet (IP) dell'utente; Informazioni indirette sulla posizione, come determinato da varie tecnologie tra cui indirizzo IP; e altre informazioni come il numero di versione dell'applicazione e cookie o simili utilizzati per raccogliere e memorizzare informazioni su un browser o dispositivo, come la lingua preferita e altre impostazioni.	ADEGUATO
Come vengono utilizzati questi dati acquisiti ?	Le informazioni personali dell'utente vengono utilizzate solo per fornire i servizi principali sopra descritti. Google si impegna a non pubblicare annunci commerciali né utilizzare le informazioni personali raccolte nell'ambito dei servizi principali per scopi pubblicitari.	ADEGUATO
Chi puo' vedere i dati acquisiti ?	Le informazioni raccolte non vengono condivise senza uno specifico consenso con nessuno al di fuori di Google se non in circostanze limitate: Con gli amministratori interni alla scuola di Google Workspace, che hanno accesso alle informazioni archiviate negli account Google degli utenti di quella scuola o dominio. Per lavorazioni esterne. Anche Google talvolta fornisce informazioni personali a suoi affiliati o ad altre aziende o persone fidate affinché le elaborino per in nome e per conto di Google, sulla base di istruzioni e in conformità con l'informativa sulla privacy. Per motivi legali. Le informazioni personali possono essere condivise con terzi qualora ciò fosse necessario per soddisfare norme giuridiche o procedimenti legali o richiesta governativa applicabile, o per applicare i termini di servizio (indagini su potenziali violazioni), o per rilevare, prevenire o affrontare frodi, problemi di sicurezza o tecnici, o ancora proteggere da danni ai diritti, alla proprietà o alla sicurezza di Google, degli utenti o del pubblico come richiesto o consentito dalla legge. I genitori degli utenti di Google Workspace nelle scuole primarie e secondarie possono accedere alle informazioni personali dei propri figli o richiederne l'eliminazione tramite l'amministratore della scuola. Se un genitore desidera interrompere qualsiasi ulteriore raccolta o utilizzo delle informazioni del proprio figlio, può richiedere che l'amministratore utilizzi i controlli del servizio a sua disposizione per limitare l'accesso dell'allievo a funzioni o servizi o eliminare completamente l'account. Per evitare che i dati possano essere intercettati, gli stessi sono trattati tramite l'utilizzo di meccanismi di conservazione e comunicazione cifrati, ai fini di garantire la minimizzazione del rischio di acceso agli stessi.	ADEGUATO
Sono adottate procedure di identificazione ed autenticazione degli utenti ?	Sì. Sono disponibili sistemi di autenticazione basati su password complesse e anche a due fattori. L'accesso alle funzionalità della piattaforma è regolato da un sistema di attivazione di account con permessi specifici, protetti da password, attivabili e modificabili dall'amministratore della piattaforma.	ADEGUATO

Sono presenti robusti processi di assegnazione agli utenti di credenziali ?	Sì. La creazione delle utenze viene eseguita dall'Istituto ad opera del soggetto interno autorizzato dalla scuola all'amministrazione della piattaforma.	ADEGUATO
Le password assegnate sono protette da una "password policies" adeguata ?	Sì, Il sistema permette di imporre che le password siano complesse (almeno 8 caratteri e composte sia da caratteri, minuscoli e maiuscoli, che da numeri) inoltre è possibile imporre una scadenza temporale alla validità della password. Tale scadenza nonché l'impostazione dell'obbligo di utilizzare password complesse è demandato all'attività del soggetto interno autorizzato dalla scuola all'amministrazione della piattaforma.	ADEGUATO
Sono definiti differenti profili di autorizzazione da attribuire ai soggetti autorizzati in modo da garantire un accesso selettivo ai dati ?	Sì, All'atto della creazione delle utenze ad opera del soggetto interno autorizzato dalla scuola all'amministrazione della piattaforma, lo stesso si preoccupa di definire delle policies di accesso esclusivo ai dati di sua pertinenze. I docenti possono accedere esclusivamente ai dati relativi agli allievi delle loro classi, gli allievi possono interagire esclusivamente con i loro compagni di classe.	ADEGUATO
I canali di trasmissione utilizzati sono sicuri sotto il profilo tecnico ?	E' in uso il protocollo TLS (Transport Layer Security) che consente di criptare e recapitare i messaggi di posta in modo sicuro, sia per il traffico in entrata che per quello in uscita, consentendo così di prevenire l'intercettazione dei messaggi durante il passaggio fra server di posta. Il rapporto Crittografia mostra il numero di messaggi criptati mediante TLS nel dominio. Google si avvale di diverse misure di sicurezza volte a garantire l'autenticità, l'integrità e la privacy dei dati in transito. Google crittografa e autentica tutti i dati in transito su uno o più livelli di rete quando i dati si spostano all'esterno dei confini fisici non controllati da Google o per conto di Google. I dati in transito all'interno di un confine fisico controllato da Google o per conto di Google sono generalmente autenticati, ma non necessariamente crittografati. A seconda della connessione effettuata, Google applica le misure di protezione predefinite ai dati in transito. Ad esempio, proteggiamo le comunicazioni tra l'utente e Google Front End (GFE) utilizzando TLS. I clienti di Google Cloud con requisiti aggiuntivi per la crittografia dei dati trasmessi su WAN possono scegliere di implementare ulteriori misure di protezione per i dati trasferiti da un utente a un'applicazione o da una macchina virtuale all'altra. Queste misure di protezione comprendono tunnel IPSec, S/MIME di Gmail, certificati SSL gestiti e Istio. Google collabora attivamente con il settore per contribuire a mettere la crittografia dei dati in transito a disposizione di tutti, ovunque. Abbiamo diversi progetti open source che incoraggiano l'uso della crittografia dei dati in transito e la sicurezza dei dati su Internet in generale, tra cui Certificate Transparency, le API di Chrome e SMTP sicuro.	ADEGUATO
Sono adottate soluzioni atte a garantire la disponibilita' dei dati ?	Google Workspace presentano solo funzionalità limitate per il ripristino dei dati perduti, distrutti o danneggiati e non dispone né delle funzionalità né dell'affidabilità delle soluzioni di backup con le quali molte attività proteggono le proprie applicazioni critiche. E' da dire tuttavia che i dati custoditi sono da intendersi come dati principalmente didattici, pertanto pur trattandosi di una voce in cui la piattaforma non eccelle, la protezione garantita può dirsi adeguata se rapportata al tipo di dato trattato.	ADEGUATO
Sono adottati sistemi di protezione perimetrale ?	L'Istituto dispone di un firewall posto a monte della rete informatica che garantisce un adeguato livello di protezione perimetrale.	ADEGUATO
Sono adottati sistemi di protezione antivirus e antimalware ?	L'Istituto dispone di un software antivirus aggiornato che garantisce un adeguato livello di protezione rispetto alla distruzione e perdita dei dati oltre ad un sistema di protezione da malware hardware (firewall). Gli utilizzatori (docenti e alunni) sono inoltre espressamente formati sull'utilizzo sicuro delle risorse elettroniche e digitali, tramite istruzioni per una efficace lotta al malware.	ADEGUATO
I software di base vengono costantemente aggiornati ?	L'Istituto dispone di un programma di assistenza tecnica informatica che comprende anche l'aggiornamento dei sistemi operativi.	ADEGUATO
Degli accessi e delle operazioni compiute viene tenuta traccia registrando i file di log ?	E' in uso un sistema di registrazione e back up dei file di log riferiti alle utenze amministrative implementato dall'Amministratore di Sistema. I file di log di Google sono a disposizione del soggetto interno autorizzato dalla scuola all'amministrazione della piattaforma.	ADEGUATO
Sono definite le istruzioni da fornire ai soggetti autorizzati al trattamento ?	La Direzione Scolastica prevede la formazione di tutti gli autorizzati al trattamento dei dati.	ADEGUATO
Sono attuate misure di formazione e sensibilizzazione degli utenti ?	La Direzione Scolastica prevede l'informazione di tutti gli utilizzatori anche mediante la condivisione di un regolamento generale destinato agli allievi ed al personale utilizzatore della piattaforma.	ADEGUATO
E' stato necessario eseguire la DPIA ?	Come evidenziato nelle righe precedenti, l'esecuzione della D.P.I.A. non deve intendersi obbligatoria in quanto il trattamento in esame non appare ad elevato rischio e le misure di sicurezza attuate appaiono adeguate, tuttavia è stata volontà	ADEGUATO

	del Titolare del trattamento, consigliato in questa direzione dal D.P.O. eseguire comunque tale analisi approfondita. In conseguenza dell'analisi le misure di sicurezza definite dalla piattaforma Google Workstation appaiono ADEGUATE. Si rammenta che le stesse devono essere mantenute tali anche ad opera dell'Istituto Scolastico mediante l'adozione ed il mantenimento delle precauzioni specifiche di pertinenza del Titolare del trattamento che agisce per mezzo del soggetto interno autorizzato dalla scuola all'amministrazione della piattaforma che è stato formalmente individuato.	

Registro T2	TRATTAMENTO ECONOMICO E GIURIDICO DEL PERSONALE

Descrizione sommaria dell'attività di trattamento	Compete all'Istituto di Istruzione, in qualità di datore di lavoro, la gestione economica e giuridica di tutto il personale dipendente, a tempo determinato e indeterminato. Essa è fatta principalmente di attività c.d. "istituzionali" che trovano ragione nella diverse normative vigenti, ma anche di attività "libere", svolte per finalità di pubblico interesse e comunque riconducibili all'attività principale, ma non espressamente previste dalle normative vigenti (la partecipazione ad un torneo, la pubblicazione a vario titolo di fotografie ed immagini etc.).	
Finalità del trattamento	RACCOLTA DEI DATI GESTIONE DEI CONTRATTI DI LAVORO A TEMPO INDETERMINATO GESTIONE DEI CONTRATTI DI LAVORO A TEMPO DETERMINATO PER LE SUPPLENZE ANNUALI E BREVI RILEVAZIONE DELLE PRESENZE ELABORAZIONE DELLE RETRIBUZIONI RICOSTRUZIONE CARRIERA, ISTRUZIONE PRATICHE DI PENSIONE E GESTIONE DEL T.F.R. GESTIONE DI DATI DI NATURA GIUDIZIARIA RIFERITI AI DIPENDENTI DENUNCE DI SINISTRI ED INFORTUNI RICHIESTE E TRASMISSIONE DI DOCUMENTI RICONDUCIBILI A VARIO TITOLO AI DIPENDENTI GESTIONE DELLE PRATICHE RELATIVE A PRESTITI PERSONALI GESTIONE DEI PROCEDIMENTI DISCIPLINARI PRATICHE DI IDONEITA'/INIDONEITA' AL LAVORO GESTIONE DELLE PRATICHE DI MOBILITA' DEL PERSONALE GESTIONE DELLA FORMAZIONE E INFORMAZIONE PERIODICA DEL PERSONALE APPLICAZIONE DELLE NORME DI IGIENE E SICUREZZA DEL LAVORO ADEMPIMENTI EX LEGGE 104 GESTIONE DEI PERMESSI SINDACALI E RELATIVI A CARICHE ELETTIVE CONSERVAZIONE SOSTITUTIVA DI TUTTI I DATI PIANIFICAZIONE DELLE ATTIVITÀ, GESTIONE DI PERMESSI, CONGEDI E FERIE GESTIONE DELLE GRADUATORIE TRASMISSIONE DATI INERENTI ALL'ESERCIZIO DEI DIRITTO DI SCIOPERO DATI DEL CASELLARIO GIUDIZIALE DETENUTI AL FINE DELLA VERIFICA DELL'ASSENZA DI PRECEDENTI SPECIFICI GESTIONE DEI DATI ACQUISITI MEDIANTE "MESSA A DISPOSIZIONE" M.A.D.	
Fonte dei dati	**Raccolti direttamente presso gli interessati**	
	LA QUASI TOTALITA' DEI DATI E' RACCOLTA DIRETTAMENTE PRESSO GLI INTERESSATI	
	Raccolti presso terzi	
	MINISTERO E UFFICI SCOLASTICI SUPERIORI RISPETTO A DATI DI NATURA ANAGRAFICA PER FINALITA' ORGANIZZATIVE AZIENDA SANITARIA CON RIFERIMENTO ALLE EMERGENZE SANITARIE IN CORSO FORZE DI POLIZIA E MAGISTRATURA PER LE QUESTIONI DI RILEVANZA PENALE O DI VOLONTARIA GIURISDIZIONE	
Base giuridica	**Dati comuni (art. 6 GDPR)**	
	CONTRATTO DI LAVORO NORMATIVA VIGENTE CONSENSO (SOLO PER I TRATTAMENTI SVOLTI SU BASE VOLONTARIA E NON STRETTAMENTE ISTITUZIONALI)	
	Dati particolari (art. 9 GDPR)	
	CONTRATTO DI LAVORO NORMATIVA VIGENTE CONSENSO (SOLO PER I TRATTAMENTI SVOLTI SU BASE VOLONTARIA E NON STRETTAMENTE ISTITUZIONALI)	
Natura dei dati oggetto di trattamento	**Comuni**	**Termine trattamento**
	DATI ANAGRAFICI CURRICULUM VITAE INFORMAZIONI RELATIVE AL TITOLO DI STUDIO	ILLIMITATO PER FASCICOLI PERSONALI
	Particolari	**Termine trattamento**
	DATI INERENTI ALLO STATO DI SALUTE CONTENUTI NEL FASCICOLO PERSONALE A VARIO TITOLO O RELATIVI AD INFORTUNI, ESONERI, PARZIALI INIDONEITA' DERIVANTI DALLA SORVEGLIANZA SANITARIA	ILLIMITATO PER FASCICOLI PERSONALI
	Giudiziari	**Termine trattamento**
	DATI DEL CASELLARIO GIUDIZIALE	ILLIMITATO PER FASCICOLI PERSONALI
Modalità di trattamento dati	I DATI VENGONO TRATTATI IN MODALITA' MISTA, SIA IN FORMATO CARTACEO CHE ELETTRONICO	
Categorie di interessati	DIPENDENTI A TEMPO DETERMINATO E INDETERMINATO, DOCENTI E APPARTENENTI AL PERSONALE A.T.A.	
Autorizzati al trattamento	**Interni**	**Trattamenti eseguiti**
	PERSONALE DELLO STAFF DEL DIRIGENTE SCOLASTICO DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI PERSONALE AMMINISTRATIVO DELLA SEGRETERIA DEL PERSONALE PERSONALE INCARICATO DI PRESTAZIONI DI ASSISTENZA INFORMATICA	RACCOLTA REGISTRAZIONE ORGANIZZAZIONE STRUTTURAZIONE CONSERVAZIONE CONSULTAZIONE ELABORAZIONE SELEZIONE RAFFRONTO UTILIZZO INTERCONNESSIONE BLOCCO COMUNICAZIONE DIFFUSIONE CANCELLAZIONE DISTRUZIONE

		ESTRAZIONE
	Esterni (Responsabili del Trattamento)	**Trattamenti eseguiti**
	PERSONALE INCARICATO DELL'ASSISTENZA INFORMATICA GESTORE DEL REGISTRO ELETTRONICO GESTORE DELLA PIATTAFORMA DI DIDATTICA A DISTANZA INCARICATO DEL RUOLO DI R.S.P.P. INCARICATO DEL RUOLO DI D.P.O. INCARICATO DEL RUOLO DI MEDICO COMPETENTE	REGISTRAZIONE ORGANIZZAZIONE STRUTTURAZIONE CONSERVAZIONE CONSULTAZIONE ELABORAZIONE SELEZIONE ESTRAZIONE RAFFRONTO UTILIZZO INTERCONNESSIONE BLOCCO COMUNICAZIONE DIFFUSIONE CANCELLAZIONE DISTRUZIONE
Strutture entro le quali avviene il trattamento dati	**Dati in formato cartaceo**	**Archiviazione storica dati cartacei**
	UFFICIO DEL DIRIGENTE SCOLASTICO E SUOI VICE SEGRETERIA DEL PERSONALE	ARCHIVIO DEL PERSONALE
	Dati in formato elettronico	**Archiviazione storica dati elettronici**
	SERVER DI SEGRETERIA CLOUD (REGISTRO ELETTRONICO) CLOUD (PIATTAFORMA DIDATTICA A DISTANZA)	UNITA' DI BACK UP DEL SERVER CONSERVATORIA DIGITALE (REGISTRO ELETTRONICO) CONSERVATORIA DIGITALE (PIATTAFORMA)
	Software impiegati per il trattamento informatico dei dati in formato elettronico	
	SOFTWARE GESTIONALE D'ISTITUTO SOFTWARE GESTIONALE MINISTERIALE	REGISTRO ELETTRONICO PIATTAFORMA DIDATTICA A DISTANZA

Possibili destinatari di attività di comunicazione	**Comunicazioni istituzionali**	**Extra UE**	**Comunicazioni su base volontaria**	**Extra UE**
	ENTI TERRITORIALI DELLO STATO AMMINISTRAZIONE SCOLASTICA I.N.A.I.L. I.N.P.S. AZIENDA SANITARIA LOCALE / A.T.S. R.S.P.P. D.P.O. MEDICO COMPETENTE ALTRI ISTITUTI SCOLASTICI RETI DI ISTITUTI (FORMAZIONE)	NO	AGENZIE VIAGGI COMPAGNIE DI ASSICURAZIONE FOTOGRAFI E VIDEOMAKER SITO INTERNET ISTITUZIONALE SOCIAL SCOLASTICI ALTRI ISTITUTI SCOLASTICI	NO
Informativa	VIENE FORNITA INFORMATIVA SPECIFICA			
Profilazione	NON VIENE ATTUATA NESSUNA ATTIVITA' DI PROFILAZIONE			
Frequenza	IL TRATTAMENTO AVVIENE CON FREQUENZA QUOTIDIANA DURANTE IL PERIODO DI ATTIVITA' SCOLASTICA			

Valutazione del rischio	**TRATTAMENTO**	**PROBABILITA' (P)**	**CONSEGUENZE (C)**	**LIVELLO DI RISCHIO (R)**
	GENERALE	POCO PROBABILE	GRAVI	**RILEVANTE**
	FIRMA GRAFOMETRICA	IMPROBABILE	GRAVI	**MEDIO BASSO**
	REGISTRO ELETTRONICO	POCO PROBABILE	GRAVI	**RILEVANTE**
	PIATTAFORMA DIDATTICA ONLINE	POCO PROBABILE	LIMITATE	**MEDIO BASSO**
	PIATTAFORMA DI LAVORO AGILE	POCO PROBABILE	GRAVI	**RILEVANTE**

Valutazione della obbligatorietà della DPIA	L'esito della valutazione dei rischi mostra un livello di rischio ELEVATO per i diritti e le libertà delle persone fisiche interessate ?	**NO**
	L'attività comporta procedimenti valutativi, di scoring o di profilazione ?	**NO**
	L'attività comporta la presa di decisioni automatizzate che producono significativi effetti giuridici (ammissioni, assunzioni, concessioni etc.) ?	**NO**
	L'attività comporta il monitoraggio sistematico di persone fisiche (videosorveglianza ad esempio) ?	**NO**
	L'attività comporta il trattamento di dati particolari, giudiziari o di natura estremamente personale (es. opinioni politiche) ?	**SI**
	L'attività comporta il trattamento di dati personali su larga scala ?	**NO**
	L'attività comporta la combinazione o il raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal contesto iniziale (big data) ?	**NO**
	L'attività comporta il trattamento di dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani etc.) ?	**NO**
	L'attività comporta utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (riconoscimento facciale ad esempio) ?	**NO**
	L'attività comporta trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).	**NO**
SI CONCLUDE LA VALUTAZIONE A FAVORE DELLA OPPORTUNITA' (NON OBBLIGO) DI ESEGUIRE LA DPIA PER QUESTO TRATTAMENTO		

Valutazione del rischio su questo trattamento a valle della DPIA	**TRATTAMENTO**	**RISCHIO INTRINSECO (Ri)**	**VULNERABILITA' (Vu)** SI CONSIDERA IL VALORE PEGGIORE	**RISCHIO NORMALIZZATO**
	GENERALE	RILEVANTE	PARZ. ADEGUATO	**RILEVANTE**
	FIRMA GRAFOMETRICA	MEDIO BASSO	ADEGUATO	**MOLTO BASSO**
	REGISTRO ELETTRONICO	RILEVANTE	ADEGUATO	**MEDIO BASSO**
	PIATTAFORMA DIDATTICA ONLINE	MEDIO BASSO	ADEGUATO	**MOLTO BASSO**
	PIATTAFORMA DI LAVORO AGILE	RILEVANTE	ADEGUATO	**MEDIO BASSO**

AL FINE DEL CONTENIMENTO DEL RISCHIO SONO ADOTTATE LE SEGUENTI MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE:

MISURA DI SICUREZZA	RISCHIO CONTRASTATO	ADEGUATEZZA (Vu)
E' adottata una politica di istituto per la sicurezza e la protezione dei dati ed all'interno dell'Istituto sono definiti i ruoli e le responsabilità di ciascuno anche mediante consegna di lettere di autorizzazione dettagliate	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	ADEGUATO
Sono utilizzati software antivirus e firewall	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (virus, accessi non autorizzati, utilizzo di supporti non autorizzati, uso non autorizzato di strumentazione, etc.).	ADEGUATO
Vengono attuati i *back up* con frequenza quotidiana	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Interruzione servizi (sbalzi di tensione, guasti all'impianto, interruzione collegamenti di rete, etc.); - Furto di dati e distruzione volontaria ed involontaria.	ADEGUATO
Sono applicate, da parte del soggetto incaricato dell'amministrazione del sistema informatico, procedure di "*disaster recovery*" che garantiscono il ripristino dell'accesso ai dati in tempi ridotti	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Interruzione servizi (sbalzi di tensione, guasti all'impianto, interruzione, collegamenti di rete, etc.); - Azioni di danneggiamento volontario.	PARZIALMENTE ADEGUATO
Sono adottati sistemi di cifratura e anonimizzazione dei dati relativi allo stato di salute delle persone	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Furto e sottrazione di dati	PARZIALMENTE ADEGUATO
Sono registrati da parte del soggetto incaricato dell'amministrazione del sistema informatico, i "*log-file*" al fine di ricostruire gli accessi ai database	- Azioni non autorizzate (errori volontari o involontari, uso non autorizzato di strumentazione, supporti etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.).	PARZIALMENTE ADEGUATO
Viene eseguita periodica manutenzione della rete informatica in cui si esegue il trattamento dei dati al fine di controllare periodicamente il funzionamento regolare di antivirus, firewall nonché assicurare l'aggiornamento dei sistemi operativi in uso e di tutti i presidi di sicurezza attiva	- Problemi tecnici (anomalie e malfunzionamento software, problemi hardware).	ADEGUATO
I Data Center di cui l'Istituto di serve sono in possesso di certificazione ISO	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware).	ADEGUATO
I singoli incaricati vengono formalmente autorizzati al trattamento dei dati ed a ciascuno vengono fornite credenziali personali (nome utente e *password*) per eseguire l'accesso ai sistemi informatici	- Azioni non autorizzate (errori volontari o involontari, protezione da virus e malware in genere, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software).	ADEGUATO
Le credenziali di autenticazione fornite ai singoli incaricati sono disattivate in caso di assenza della persona prolungata per oltre 6 mesi	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica etc. da parte di soggetti non più autorizzati); - Azioni non autorizzate (errori volontari o involontari, uso non autorizzato di strumentazione, etc.).	ADEGUATO
Le credenziali di autenticazione fornite ai singoli incaricati sono disattivate o i profili di accesso sono modificati per colui che, a causa di un cambiamento di mansione, perda la possibilità di trattare i dati o se la veda modificata	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica etc. da parte di soggetti non più autorizzati); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	ADEGUATO
I sistemi di autorizzazione prevedono la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc. eseguita da parte dichi non è più autorizzato a trattare i dati).	ADEGUATO

Le parole chiave (*password*) fornite sono complesse (lunghe almeno 8 caratteri e formate da lettere e numeri, maiuscole e minuscole) e non sono riferibili a condizioni personali dell'autorizzato. **Le password devono essere modificate la primo accesso e devono essere cambiate ogni 3 mesi**	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Evitare che l'accesso ai dati digitali possa avvenire troppo facilmente.	ADEGUATO
Esclusivamente ai singoli incaricati viene concesso l'accesso ai locali (uffici, sale docenti, archivi, CED etc.) ed agli arredi (cassetti, armadi, schedari etc.) in cui devono prestare la loro attività di trattamento	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Evitare che l'accesso ai dati cartacei ed agli elaboratori possa avvenire troppo facilmente.	ADEGUATO
I locali in cui avviene il trattamento dati sono dotati di presidi antincendio	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.);	ADEGUATO
Le prese di alimentazione elettrica a cui sono connessi gli apparati informatici di rete nonché server ed elaboratori forniscono idonee garanzie di stabilità	- Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Interruzione servizi (sbalzi di tensione, guasti all'impianto, interruzione collegamenti di rete, etc.).	ADEGUATO
I locali in cui avviene il trattamento dati, al termine dell'attività, vengono chiusi a chiave così come cassetti ed armadi contenenti dati personali, le chiavi sono nella disponibilità di soli soggetti autorizzati a detenerle	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware).	ADEGUATO
I supporti cartacei contenenti dati personali non più necessari vengono distrutti fisicamente prima della loro eliminazione	- Accesso da parte di soggetti non autorizzati;	ADEGUATO
I supporti magnetici (chiavette, dischi removibili etc.) contenenti dati personali non più necessari vengono distrutti fisicamente prima della loro eliminazione	- Accesso da parte di soggetti non autorizzati;	ADEGUATO
Ai singoli utenti autorizzati vengono fornite istruzioni per la custodia e l'uso di supporti removibili	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Perdita, smarrimento, furto.	ADEGUATO
E' prevista l'organizzazione periodica di corsi di formazione ed interventi informativi volti a fornire nozioni ed a sensibilizzare il personale autorizzato	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Perdita, smarrimento.	ADEGUATO
Il personale autorizzato è soggetto alla vigilanza del Titolare del trattamento e degli altri autorizzati con compiti di coordinamento e direttivi	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Furti, danneggiamenti volontari; - Uso non autorizzato di supporti personali; - Uso illegale di software.	ADEGUATO
Tutte le procedure sono oggetto di riesame almeno annuale in occasione dell'audit periodico eseguito dal D.P.O.	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Verifica della corretta applicazione delle norme regolamentari.	ADEGUATO
I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	ADEGUATO
Sono definiti termini di conservazione e le condizioni di impiego e successiva distruzione dei dati personali trattati	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.).	ADEGUATO
Ancorché non obbligatoria, su questo trattamento viene eseguita la DPIA (Data Protection Impact Assesment)	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	ADEGUATO

Registro T3	**TRATTAMENTO DEI DATI DEI FORNITORI ED ASSIMILATI**

Descrizione sommaria dell'attività di trattamento	L'Istituto Scolastico, nell'esercizio della propria autonomia, agisce come un soggetto di diritto privato e conseguentemente intrattiene rapporti di natura commerciale con fornitori di beni e di servizi. L'individuazione dei fornitori avviene mediante procedure definite nel codice degli appalti e con obblighi di trasparenza peculiari.			
Finalità del trattamento	RACCOLTA DEI DATI DI FORNITORI – ESPERTI, SPECIALISTI E VOLONTARI GESTIONE DEI CONTRATTI DI FORNITURA DI BENI E SERVIZI GESTIONE DEI COLLAUDI ELABORAZIONE DEI PAGAMENTI AI FORNITORI GESTIONE DI DATI DI NATURA GIUDIZIARIA RIFERITI AGLI AMMINISTRATORI ED AI DIPENDENTI DEI FORNITORI DENUNCE DI SINISTRI ED INFORTUNI RICHIESTE E TRASMISSIONE DI DOCUMENTI APPLICAZIONE DELLE NORME DI IGIENE E SICUREZZA DEL LAVORO CONSERVAZIONE SOSTITUTIVA DI TUTTI I DATI GESTIONE DEI BANDI DI GARA E DELLE PROCEDURE PREVISTE DAL CODICE DEGLI APPALTI APPLICAZIONE DEGLI OBBLIGHI DI TRASPARENZA AMMINISTRATIVA DATI DEL CASELLARIO GIUDIZIALE DETENUTI AL FINE DELLA VERIFICA DELL'ASSENZA DI PRECEDENTI SPECIFICI			
Fonte dei dati	**Raccolti direttamente presso gli interessati**			
	LA QUASI TOTALITA' DEI DATI E' RACCOLTA DIRETTAMENTE PRESSO GLI INTERESSATI			
	Raccolti presso terzi			
	AMMINISTRAZIONI LOCALI DELLO STATO AMMINISTRAZIONE SCOLASTICA CASELLARIO GIUDIZIALE			
Base giuridica	**Dati comuni (art. 6 GDPR)**			
	CONTRATTO			
	Dati particolari (art. 9 GDPR)			
	NESSUNA			
Natura dei dati oggetto di trattamento	**Comuni**	**Termine trattamento**		
	DATI ANAGRAFICI DI AMMINISTRATORI, SPECIALISTI, ESPERTI E DATI IDENTIFICATIVI DELLE SOCIETA' DATI CONTABILI ED AMMINISTRATIVI	ILLIMITATO PER I DATI AMMINISTRATIVI 10 ANNI PER TUTTI I DATI CONTABILI		
	Particolari	**Termine trattamento**		
	NESSUNO	NESSUNO		
	Giudiziari	**Termine trattamento**		
	DATI DEL CASELLARIO GIUDIZIALE	ILLIMITATO PER I DATI AMMINISTRATIVI		
Modalità di trattamento dati	I DATI VENGONO TRATTATI IN MODALITA' MISTA, SIA IN FORMATO CARTACEO CHE ELETTRONICO			
Categorie di interessati	FORNITORI DI BENI E SERVIZI, SPECIALISTI ESTERNI, ESPERTI ESTERNI, VOLONTARI			
Autorizzati al trattamento	**Interni**	**Trattamenti eseguiti**		
	PERSONALE DELLO STAFF DEL DIRIGENTE SCOLASTICO DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI PERSONALE AMMINISTRATIVO DELLA SEGRETERIA CONTABILE PERSONALE INCARICATO DI PRESTAZIONI DI ASSISTENZA INFORMATICA	RACCOLTA REGISTRAZIONE ORGANIZZAZIONE STRUTTURAZIONE CONSERVAZIONE CONSULTAZIONE ELABORAZIONE SELEZIONE ESTRAZIONE	RAFFRONTO UTILIZZO INTERCONNESSIONE BLOCCO COMUNICAZIONE DIFFUSIONE CANCELLAZIONE DISTRUZIONE	
	Esterni (Responsabili del Trattamento)	**Trattamenti eseguiti**		
	PERSONALE INCARICATO DELL'ASSISTENZA INFORMATICA INCARICATO DEL RUOLO DI R.S.P.P. INCARICATO DEL RUOLO DI D.P.O. INCARICATO DEL RUOLO DI MEDICO COMPETENTE	REGISTRAZIONE ORGANIZZAZIONE STRUTTURAZIONE CONSERVAZIONE CONSULTAZIONE ELABORAZIONE SELEZIONE ESTRAZIONE	RAFFRONTO UTILIZZO INTERCONNESSIONE BLOCCO COMUNICAZIONE DIFFUSIONE CANCELLAZIONE DISTRUZIONE	
Strutture entro le quali avviene il trattamento dati	**Dati in formato cartaceo**	**Archiviazione storica dati cartacei**		
	UFFICIO DEL DIRIGENTE SCOLASTICO E SUOI VICE SEGRETERIA CONTABILE	ARCHIVIO AMMINISTRATIVO		
	Dati in formato elettronico	**Archiviazione storica dati elettronici**		
	SERVER DI SEGRETERIA	UNITA' DI BACK UP DEL SERVER		
	Software impiegati per il trattamento informatico dei dati in formato elettronico			
	SOFTWARE GESTIONALE D'ISTITUTO SOFTWARE GESTIONALE MINISTERIALE	REGISTRO ELETTRONICO PIATTAFORMA DIDATTICA A DISTANZA		
	Comunicazioni istituzionali	**Extra UE**	**Comunicazioni su base volontaria**	**Extra UE**

Possibili destinatari di attività di comunicazione	ENTI TERRITORIALI DELLO STATO AMMINISTRAZIONE SCOLASTICA AZIENDA SANITARIA LOCALE / A.T.S. R.S.P.P. D.P.O. MEDICO COMPETENTE	NO	COMPAGNIE DI ASSICURAZIONE	NO
Informativa	VIENE FORNITA INFORMATIVA SPECIFICA			
Profilazione	NON VIENE ATTUATA NESSUNA ATTIVITA' DI PROFILAZIONE			
Frequenza	IL TRATTAMENTO AVVIENE CON FREQUENZA QUOTIDIANA			

Valutazione del rischio	**TRATTAMENTO**	**PROBABILITA' (P)**	**CONSEGUENZE (C)**	**LIVELLO DI RISCHIO (R)**
	GENERALE	POCO PROBABILE	LIMITATE	**MEDIO BASSO**
	FIRMA GRAFOMETRICA	IMPROBABILE	GRAVI	**MEDIO BASSO**
	REGISTRO ELETTRONICO	POCO PROBABILE	LIMITATE	**MEDIO BASSO**
	PIATTAFORMA DIDATTICA ONLINE	POCO PROBABILE	LIMITATE	**MEDIO BASSO**

Valutazione della obbligatorietà della DPIA	L'esito della valutazione dei rischi mostra un livello di rischio ELEVATO per i diritti e le libertà delle persone fisiche interessate ?	**NO**
	L'attività comporta procedimenti valutativi, di scoring o di profilazione ?	**NO**
	L'attività comporta la presa di decisioni automatizzate che producono significativi effetti giuridici (ammissioni, assunzioni, concessioni etc.) ?	**NO**
	L'attività comporta il monitoraggio sistematico di persone fisiche (videosorveglianza ad esempio) ?	**NO**
	L'attività comporta il trattamento di dati particolari, giudiziari o di natura estremamente personale (es. opinioni politiche) ?	**NO**
	L'attività comporta il trattamento di dati personali su larga scala ?	**NO**
	L'attività comporta la combinazione o il raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal contesto iniziale (big data) ?	**NO**
	L'attività comporta il trattamento di dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani etc.) ?	**NO**
	L'attività comporta utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (riconoscimento facciale ad esempio) ?	**NO**
	L'attività comporta trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).	**NO**
SI CONCLUDE LA VALUTAZIONE A FAVORE DEL NON OBBLIGO DI ESEGUIRE LA DPIA PER QUESTO TRATTAMENTO		

Valutazione del rischio su questo trattamento a valle della DPIA	**TRATTAMENTO**	**RISCHIO INTRINSECO (Ri)**	**VULNERABILITA' (Vu)** SI CONSIDERA IL VALORE PEGGIORE	**RISCHIO NORMALIZZATO**
	GENERALE	MEDIO BASSO		**MEDIO BASSO**
	FIRMA GRAFOMETRICA	MEDIO BASSO		**MEDIO BASSO**
	REGISTRO ELETTRONICO	MEDIO BASSO		**MEDIO BASSO**
	PIATTAFORMA DIDATTICA ONLINE	MEDIO BASSO		**MEDIO BASSO**

AL FINE DEL CONTENIMENTO DEL RISCHIO SONO ADOTTATE LE SEGUENTI MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE:

MISURA DI SICUREZZA	RISCHIO CONTRASTATO	ADEGUATEZZA (Vu)
E' adottata una politica di istituto per la sicurezza e la protezione dei dati ed all'interno dell'Istituto sono definiti i ruoli e le responsabilità di ciascuno anche mediante consegna di lettere di autorizzazione dettagliate	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	
Sono utilizzati software antivirus e firewall	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (virus, accessi non autorizzati, utilizzo di supporti non autorizzati, uso non autorizzato di strumentazione, etc.).	
Vengono attuati i *back up* con frequenza quotidiana	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Interruzione servizi (sbalzi di tensione, guasti all'impianto, interruzione collegamenti di rete, etc.); - Furto di dati e distruzione volontaria ed involontaria.	
Sono applicate, da parte del soggetto incaricato dell'amministrazione del sistema informatico, procedure di "*disaster recovery*" che garantiscono il ripristino dell'accesso ai dati in tempi ridotti	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Interruzione servizi (sbalzi di tensione, guasti all'impianto, interruzione, collegamenti di rete, etc.); - Azioni di danneggiamento volontario.	
Sono adottati sistemi di cifratura e anonimizzazione dei dati relativi allo stato di salute delle persone	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni,	

	infiltrazioni in messaggistica di posta elettronica, etc.); - Furto e sottrazione di dati	
Sono registrati da parte del soggetto incaricato dell'amministrazione del sistema informatico, i "*log-file*" al fine di ricostruire gli accessi ai database	- Azioni non autorizzate (errori volontari o involontari, uso non autorizzato di strumentazione, supporti etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.).	
Viene eseguita periodica manutenzione della rete informatica in cui si esegue il trattamento dei dati al fine di controllare periodicamente il funzionamento regolare di antivirus, firewall nonché assicurare l'aggiornamento dei sistemi operativi in uso e di tutti i presidi di sicurezza attiva	- Problemi tecnici (anomalie e malfunzionamento software, problemi hardware).	
I Data Center di cui l'Istituto di serve sono in possesso di certificazione ISO	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware).	
I singoli incaricati vengono formalmente autorizzati al trattamento dei dati ed a ciascuno vengono fornite credenziali personali (nome utente e *password*) per eseguire l'accesso ai sistemi informatici	- Azioni non autorizzate (errori volontari o involontari, protezione da virus e MALWARE in genere, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software).	
Le credenziali di autenticazione fornite ai singoli incaricati sono disattivate in caso di assenza della persona prolungata per oltre 6 mesi	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica etc. da parte di soggetti non più autorizzati); - Azioni non autorizzate (errori volontari o involontari, uso non autorizzato di strumentazione, etc.).	
Le credenziali di autenticazione fornite ai singoli incaricati sono disattivate o i profili di accesso sono modificati per colui che, a causa di un cambiamento di mansione, perda la possibilità di trattare i dati o se la veda modificata	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica etc. da parte di soggetti non più autorizzati); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	
I sistemi di autorizzazione prevedono la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc. eseguita da parte dichi non è più autorizzato a trattare i dati).	
Le parole chiave (*password*) fornite sono complesse (lunghe almeno 8 caratteri e formate da lettere e numeri, maiuscole e minuscole) e non sono riferibili a condizioni personali dell'autorizzato. Le password devono essere modificate la primo accesso e devono essere cambiate ogni 3 mesi	- Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Evitare che l'accesso ai dati digitali possa avvenire troppo facilmente.	
Esclusivamente ai singoli incaricati viene concesso l'accesso ai locali (uffici, sale docenti, archivi, CED etc.) ed agli arredi (cassetti, armadi, schedari etc.) in cui devono prestare la loro attività di trattamento	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Evitare che l'accesso ai dati cartacei ed agli elaboratori possa avvenire troppo facilmente.	
I locali in cui avviene il trattamento dati sono dotati di presidi antincendio	- Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.);	
Le prese di alimentazione elettrica a cui sono connessi gli apparati informatici di rete nonché server ed elaboratori forniscono idonee garanzie di stabilità	- Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Interruzione servizi (sbalzi di tensione, guasti all'impianto, interruzione collegamenti di rete, etc.).	
I locali in cui avviene il trattamento dati, al termine dell'attività, vengono chiusi a chiave così come cassetti ed armadi contenenti dati personali, le	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware).	

chiavi sono nella disponibilità di soli soggetti autorizzati a detenerle		
I supporti cartacei contenenti dati personali non più necessari vengono distrutti fisicamente prima della loro eliminazione	- Accesso da parte di soggetti non autorizzati;	
I supporti magnetici (chiavette, dischi removibili etc.) contenenti dati personali non più necessari vengono distrutti fisicamente prima della loro eliminazione	- Accesso da parte di soggetti non autorizzati;	
Ai singoli utenti autorizzati vengono fornite istruzioni per la custodia e l'uso di supporti removibili	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Eventi naturali ed agenti fisici (terremoti, incendi, allagamenti etc.); - Perdita, smarrimento, furto.	
E' prevista l'organizzazione periodica di corsi di formazione ed interventi informativi volti a fornire nozioni ed a sensibilizzare il personale autorizzato	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Perdita, smarrimento.	
Il personale autorizzato è soggetto alla vigilanza del Titolare del trattamento e degli altri autorizzati con compiti di coordinamento e direttivi	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Furti, danneggiamenti volontari; - Uso non autorizzato di supporti personali; - Uso illegale di software.	
Tutte le procedure sono oggetto di riesame almeno annuale in occasione dell'audit periodico eseguito dal D.P.O.	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.); - Problemi tecnici (anomalie e malfunzionamento software, problemi hardware); - Verifica della corretta applicazione delle norme regolamentari.	
I dati non sono diffusi o comunicati a terzi al di fuori delle specifiche previsioni normative	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.).	
Sono definiti termini di conservazione e le condizioni di impiego e successiva distruzione dei dati personali trattati	- Azioni non autorizzate (errori volontari o involontari, virus, uso non autorizzato di strumentazione, etc.); - Compromissione delle informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, etc.).	

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

VI. 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'ente 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 scolastiche.
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 particolari 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

Ancorché si tratti di una pratica oggetto di progressiva dismissione, 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]

VII. 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, in tali casi al soggetto incaricato spetta solo il compito di verificare che il salvataggio abbia avuto buon fine.

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.
La modalità di back-up cosiddetta "in cloud" ossia che avvenga utilizzando una piattaforma remota accessibile mediante web, non modifica i tratti essenziali della procedura che dovrà essere sempre verificata in ordine alla puntuale esecuzione del trasferimento dei dati oggetto di *back up*.

VIII. 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 autorizzate al 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.

IX. 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.

X. 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.

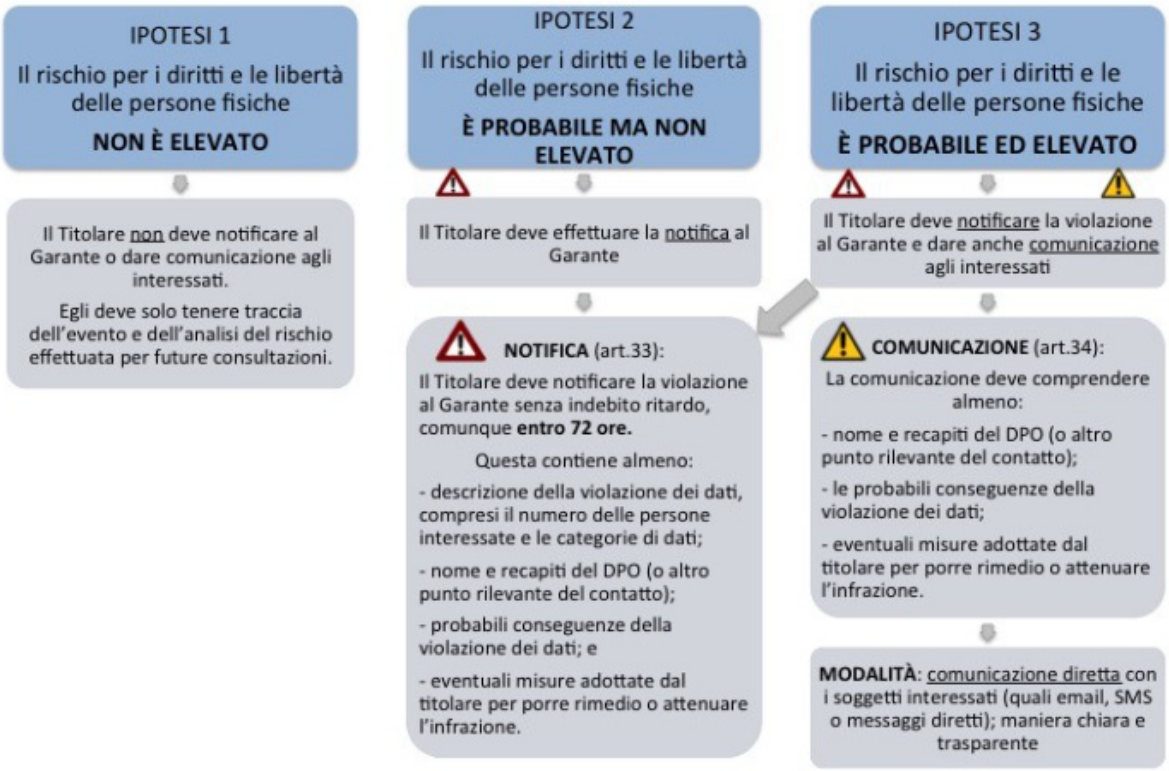
TIPO DI VIOLAZIONE (BREACH)	DEFINIZIONE	SOGLIA DI SEGNALAZIONE	ESEMPI (segnalazione SI)	CONTROESEMPI (segnalazione NO)
DISTRUZIONE	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del Titolare. In caso di richiesta del dato da parte dell'interessato 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.

XI. 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.

XII. FORMAZIONE DEGLI AUTORIZZATI

Al Titolare del trattamento dei dati è affidato il compito di verificare annualmente le necessità di formazione del personale autorizzato ad eseguire i compiti indicati nella lettera di autorizzazione.
Per ogni autorizzato al trattamento il Titolare 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 autorizzati 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 AUTORIZZAZIONE" - Analisi dei rischi collegati alle attività proprie della categoria - Organizzazione e procedure di sicurezza	TITOLARE DEL TRATTAMENTO RESPONSABILE DEL TRATTAMENTO AUTORIZZATI AL 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 AUTORIZZAZIONE" - 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

XIII. 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

_____