Istituto Comprensivo di Traona
Costiera dei Cech

Ministero dell'Istruzione, dell'Università e della Ricerca
ISTITUTO COMPRENSIVO DI TRAONA
Via Aldo Moro n. 6 - 23019 TRAONA (SO) - Tel. 0342 653340
Codice Fiscale: 82003850144 - Codice Ufficio Univoco UFZVHU
e-mail: SOIC81200L@ISTRUZIONE.IT - SOIC81200L@PEC.ISTRUZIONE.IT
sito web: www.ictraona.it

PON 2014-2020
Unione Europea

Sezione Amministrazione Trasparente
Al DSGA
Agli Atti

OGGETTO Adozione del Registro degli incidenti informatici e delle violazioni dei dati, del Modello organizzativo e disposizioni operative del Registro delle Attività di Trattamento, ai sensi dell'art. 30 del Regolamento UE 2016/679

IL DIRIGENTE

CONSIDERATO che il 27.04.2016 è stato approvato dal Parlamento Europeo e dal Consiglio il Regolamento UE 679/2016 (GDPR – General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione Europea.

CONSIDERATO che il Regolamento UE 679/2016 è entrato in vigore in piena applicazione in data 25 maggio 2018.

CONSIDERATO che il Regolamento prevede all'art. 30 che ciascun titolare di trattamenti adotti un registro per le attività di trattamento di dati personali svolte sotto la propria responsabilità.

RITENUTO necessario ed opportuno stabilire modalità organizzative, misure procedimentali e regole di dettaglio, finalizzate anche ad omogeneizzare questioni interpretative, che permettano a questa istituzione scolastica di poter agire con adeguata funzionalità ed efficacia nell'attivazione delle disposizioni introdotte da Regolemento UE.

DETERMINA

di adottare il Registro degli incidenti informatici e delle violazioni dei dati (Allegato 1), il Modello organizzativo e disposizioni operative (Allegato 2) e il Registro delle Attività di Trattamento (Allegato 3), ai sensi dell'art. 30 del Regolamento UE 679/2016.Traona, 01.02.2019

IL DIRIGENTE SCOLASTICO
Marco Vaninetti
Documento firmato digitalmente ai sensi del c.d. Codice dell'Amministrazione Digitale e norme ad esso connesse

Modello Organizzativo e Disposizioni Operative per l'adeguamento al GDPR (Reg. UE 2016/679) e per l'impostazione di un Sistema per la Gestione della Sicurezza delle Informazioni secondo gli standard internazionali ISO 27001 e 27002

Nome documento:	Modello Organizzativo e Disposizioni Operative per l'adeguamento al Regolamento UE 2016/679 (GDPR) e per l'impostazione di un Sistema per la Gestione della Sicurezza delle Informazioni
Codice documento:	IC e IS – Reg Adeguamento GDPR Ver 1-0.doc
Nome file:	IC e IS – Reg Adeguamento GDPR Ver 1-0.doc
Stato documento:	Definitivo
Versione:	1.0
Data creazione:	28 maggio 2018
Data ultimo aggiornamento	2 luglio 2018

Indice

SEZIONE 1 – PARTE GENERALE

Art. 1 - Premessa

Il regolamento europeo Reg. 2016/679 ("GDPR" – General Data Protection regulation), in quanto regolamento e non direttiva, è immediatamente esecutivo e pertanto non necessita di alcun recepimento o approvazione.

Il presente regolamento pertanto non concerne il recepimento del GDPR, cosa che non avrebbe alcun senso ne' da un punto di vista concettuale, ne' dal punto di vista pratico.

Tuttavia, il GDPR in alcuni punti (es. art 32 – sicurezza del trattamento) enuncia delle affermazioni di principio o degli obiettivi da raggiungere, lasciando ampio margine discrezionale sulle modalità concrete attraverso le quali gli obiettivi possono venire raggiunti.

Modalità che dipendono da molteplici fattori, tra i quali le dimensioni, l'organizzazione, la cultura, le competenze e le dotazioni dell'Ente.

Il presente documento serve pertanto a individuare con precisione le modalità, le prassi, la metodologia, le tecniche e gli strumenti mediante le quali, nell'ambito specifico dell'Istituto, si raggiunge e si mantiene nel tempo l'adeguamento e la conformità alle prescrizioni del GDPR e si imposta un SGSI – Sistema per la Gestione della Sicurezza delle Informazioni e si possa dimostrare, in caso di controlli o ispezioni da parte degli organismi preposti, che l'Istituto è in regola con le prescrizioni del succitato Regolamento UE 2016/679.

Art. 2 - Obiettivo del presente Regolamento

Il presente regolamento permette di raggiungere i seguenti obiettivi:

- implementare il principio fondamentale di responsabilizzazione ("accountability") introdotto dal GDPR, in base al quale il titolare deve

non solo essere conforme alle prescrizioni del GDPR, ma deve anche essere in grado di dimostrare la conformità raggiunta;

- indicare metodologie e prassi operative specifiche per l'adeguamento alle prescrizioni del GDPR, tenendo conto del contesto specifico dell'Ente;
- in particolare, per quanto riguarda la sicurezza (art. 32), individuare precisamente una procedura per testare, verificare periodicamente e valutare regolarmente l'efficacia delle misure tecniche ed organizzative da mettere in atto per assicurare un adeguato livello di sicurezza e di protezione dei dati
- impostare un SGSI – Sistema di Gestione della Sicurezza delle Informazioni che permetta di dimostrare che l'Istituto è conforme ai requisiti di sicurezza previsti dall'art. 32 del GDPR e conforme a riconosciuti standard di sicurezza a livello internazionale.

Art. 3 - Liceità dei trattamenti

Per ciascun trattamento effettuato, deve essere verificata e documentata per iscritto la liceità del trattamento stesso; nel caso di un soggetto pubblico come l'Istituto, la liceità del trattamento deve essere individuata nella base giuridica che giustifica/richiede il trattamento specifico.

La base giuridica deve essere può essere costituita da:

- funzioni istituzionali dell'Ente, oppure
- norme di legge di rango primario.

Si dovrà inoltre verificare che non sussistano norme di legge che vietino esplicitamente il trattamento.

Art. 4 - Informativa agli interessati

Il GDPR prevede che, oltre a quanto già previsto dall'art. 13 del D.Lgs. 196/2003, l'informativa contenga le seguenti informazioni:

- i dati di contatto del responsabile della protezione dei dati
- la base giuridica del trattamento
- il tempo di conservazione dei dati personali o, se non è possibile, i criteri utilizzati per determinare tale periodo
- gli ulteriori diritti dell'interessato introdotti dal GDPR.

Art. 5 - Consenso al trattamento dei dati

Il GDPR mantiene un principio chiave introdotto dall'art. 18 del D.Lgs. 196/2003, e cioè che i soggetti pubblici non devono richiedere il consenso dell'interessato. Pertanto, sia nei moduli cartacei che nei form web, non si dovrà chiedere il consenso dell'interessato (mentre invece è necessario fornire l'informativa).

In via del tutto residuale, è consentito che l'Istituto possa chiedere il consenso dei genitori, laddove trattasi di servizi opzionali, di cui i genitori o tutori degli alunni potrebbero decidere di non usufruire; in tali casi tuttavia, il consenso ha di fatto la valenza di documentare e tenere traccia del fatto che la famiglia/il tutore ha deciso di usufruire del servizio. Tali casistiche residuali sono precisamente individuate e codificate, e si possono ricondurre alle tre seguenti fattispecie:

- decisione di avvalersi del servizio di ristorazione scolastica
- decisione di partecipare a gite scolastiche, e di conseguenza di aderire a forme di assicurazione
- decisione di avvalersi del servizio di trasporto scolastico, e di conseguenza di aderire a forme di assicurazione.

Art. 6 - Incaricati del trattamento dei dati

Mentre il D.Lgs. 196/2003 prevedeva esplicitamente la figura dell'incaricato del trattamento dei dati, il GDPR tratta la figura dell'incaricato in termini più generali, all'art. 29 – Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento, laddove specifica che "il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali, non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri. Nel caso dell'Istituto, per chiarezza si continuerà ad usare la dicitura "Incaricato del trattamento dei dati", intendendo con tale locuzione i soggetti di cui all'art. 29 del GDPR. Ai fini del GDPR, continuano ad essere valide le preesistenti nomine ad incaricato del trattamento dei dati, che si intendono rinnovate ai sensi dell'art. 29 del GDPR. E' data comunque facoltà di integrare o modificare o revocare esplicitamente le preesistenti nomine ad incaricato del trattamento dei dati, oppure di emettere nuovi atti di nomina secondo i quali le persone fisiche vengono denominati soggetti "designati" ai sensi del GDPR.

Art. 7 - Non applicabilità del requisito della portabilità dei dati

L'art. 20 del GDPR prevede astrattamente il diritto dal parte dell'interessato alla portabilità dei dati. Tuttavia l'Istituto non è tenuto a soddisfare le richieste di portabilità dei dati, in quanto:

- la portabilità dei dati non si applica ai dati in formato cartaceo
- la portabilità dei dati non si applica ai trattamenti che prescindono dal consenso.

Art. 8 - Tempi di conservazione dei dati e regole di scarto

Per quanto riguarda i tempi di conservazione dei dati e le relative regole di scarto, si applicano le prescrizioni emesse dalla articolazione regionale di riferimento della Soprintendenza Archivistica e/o quelle recepite a livello di Regolamento di Protocollo e di Manuale per la Gestione dei Flussi Documentali.

Art. 9 - Responsabili del trattamento

Il GDPR ha introdotto una significativa novità a livello organizzativo, consistente nel fatto che i tradizionali responsabili "interni" del trattamento dei dati non possono più essere designati.

L'art. 28 del GDPR prevede una figura di "responsabile del trattamento" che può essere ricoperta solo da soggetti esterni.

Alla luce di quanto detto sopra, a seconda della tipologia di dati trattati e dei trattamenti effettuati, è possibile designare in qualità di Responsabile esterno del trattamento dei dati il soggetto esterno all'Ente coinvolto a vario titolo nelle varie operazioni di trattamento dei dati, come ad esempio ditte incaricate dei servizi di assistenza e manutenzione dei degli apparati hardware oppure delle piattaforme software, con particolare riferimento alle piattaforme in cloud (es. registro elettronico, protocollo informatico in cloud, etc.).

SEZIONE 2 – SICUREZZA

Art. 10 - Obbligo di notificazione immediata di una violazione dei dati al Responsabile della protezione dei dati

Nel caso si verifichi un qualsiasi tipo di violazione dei dati, o se ne abbia anche solamente il sospetto, ne deve essere data immediata comunicazione al Dirigente Scolastico e al Responsabile della protezione dei dati, il quale si attiverà immediatamente per valutare se vi sia stata effettivamente una violazione, la portata e le conseguenze, e valutare se sussistano i presupposti per effettuare la notificazione entro 72 ore all'autorità di controllo.

Art. 11 - Registro delle violazioni dei dati

Coerentemente con quanto previsto dall'art. 33 comma 5, deve essere in ogni caso tenuto un registro di tutte le violazioni di dati verificatesi, a prescindere dal fatto che siano state notificate all'autorità di controllo. Il suddetto registro deve contenere come minimo le seguenti informazioni:

- data della violazione
- descrizione delle circostanze e dell'evento
- tipologia e quantità di interessati impattati
- conseguenze della violazione
- data di comunicazione della violazione al Garante per la protezione dei dati (se la comunicazione è stata effettuata).

Art. 12 - Il modello MMS – Modello per il Monitoraggio della Sicurezza

La sicurezza può continuamente essere compromessa da una serie di eventi che possono accadere. Questi eventi devono pertanto essere tracciati ed essere oggetto di analisi periodica.

La tracciatura degli eventi si effettua compilando il Modello MMS – Modello per il Monitoraggio della Sicurezza, con frequenza settimanale; il modello compilato deve essere inviato al Responsabile della protezione dei dati designato ai sensi dell'art. 37 del GDPR.

Art. 13 - Il modello DMS – Documento sul Monitoraggio della Sicurezza

Gli eventi di cui all'articolo precedente devono essere analizzati con frequenza almeno trimestrale, all'interno di un documento denominato MMS – Documento per il Monitoraggio della Sicurezza, predisposto dal Responsabile della protezione dei dati e posto all'attenzione del Dirigente Scolastico e del Comitato per la Sicurezza e la Privacy. All'interno del DMS devono inoltre trovare trattazione esaustiva ed organica tutte le problematiche relative alla sicurezza e alla protezione dei dati personali che si sono verificate nel trimestre di riferimento, come ad esempio:

- l'esternalizzazione di un nuovo trattamento di dati
- la predisposizione di una procedura operativa o di un regolamento ad-hoc
- la predisposizione di una lettera di nomina
- la predisposizione di una nuova informativa
- la predisposizione di comunicazioni ai dipendenti o agli interessati
- il recepimento di norme o linee guida emesse a livello nazionale od europeo, concernenti la sicurezza o la protezione dei dati

- l'analisi di una richiesta di accesso ai dati
- la revisione dei Registri del trattamenti dei dati
- lo svolgimento di un DPIA – Data Protection Impact Assessment
- la verifica del soddisfacimento dei principi di Privacy by Design e Privacy by default all'interno di un sistema o di un processo

Art. 14 - Requisiti per il raggiungimento di un adeguato livello di sicurezza nei trattamenti effettuati

Poiché l'art. 32 del GDPR lascia un ampio margine di discrezione sulle prassi da mettere in atto per assicurare un adeguato livello di sicurezza, in fase di prima applicazione del GDPR e per un periodo transitorio di 24 mesi a far data dal 25 maggio 2018, dovranno comunque essere messe in atto le misure minime di sicurezza previste dagli artt. 33, 34 e 35 del D.Lgs. 196/2003, nei modi previsti dal Disciplinare Tecnico (Allegato B al D.Lgs. 196/2003), nonché le misure minime di sicurezza per tutte le PA previste dalla Circolare AGID 2/2017.

Parimenti, in fase di prima applicazione del GDPR e per un periodo di 24 mesi a far data dal 25 maggio 2018, si dovranno seguire le prescrizioni dell'atto di natura regolamentare adottato dall'Ente ai sensi degli artt. 20 e 21 del D.Lgs. 196/2003.

Art. 15 - Il Comitato SP – Comitato per la Sicurezza e la Privacy

Per assicurare un adeguato livello di attenzione e di potere decisionale in merito a tutte le questioni riguardanti la sicurezza e la protezione dei dati personali, deve essere costituito un Comitato per la Sicurezza e la Privacy (per brevità denominato "Comitato SP"), costituito dai seguenti membri permanenti:

- Dirigente Scolastico

- D.S.G.A. o soggetto equivalente per gli Istituti parificati
- Responsabile della protezione dei dati.

Il suddetto Comitato si deve riunire con frequenza almeno semestrale (ogni sei mesi), per analizzare tutte le problematiche inerenti la sicurezza e la privacy che si sono verificate nel periodo di riferimento e analizzare tutti i modelli MMS e DMS prodotti. Alla fine di ogni riunione del Comitato deve essere prodotto a cura del DPO un verbale delle principale decisioni prese.

Art. 16 - Dimostrazione della conformità ai requisiti di sicurezza previsti dall'art. 32 del GDPR

In caso di verifiche da parte del Garante per la protezione dei dati o della Guardia di Finanza o delle autorità preposte, L'Istituto deve essere in grado di dimostrare che ha messo in atto un sistema di gestione della sicurezza tale da soddisfare i requisiti previsti dall'art. 32 del GDPR.

A tal fine è di fondamentale importanza quanto enunciato dall'art. 32 comma 3 del GDPR, laddove si specifica che l'adesione a codici di condotta approvati o ad uno scherma di certificazione può essere addotto come elemento per comprovare la conformità ed un adeguato livello di sicurezza e di protezione dei dati.

Art. 17 - Verifiche e certificazioni periodiche da parte del Responsabile della protezione dei dati

In ottemperanza a quanto previsto dagli artt. 37, 38 e 39 del GDPR, il Responsabile della protezione dei dati è tenuto ad effettuare, con frequenza almeno quadrimestrale, verifiche finalizzate a verificare e certificare il fatto che i trattamenti e le prassi messe in atto dall'Istituto sono conformi a quanto prescritto dal GDPR; oppure, in caso di non conformità, il Responsabile della protezione dei dati è tenuto

a documentare le non conformità riscontrate e ad individuare e descrivere le misure correttive da mettere in atto, specificando inoltre il termine entro il quale le suddette misure devono essere messe in atto e i soggetti coinvolti.

Art. 18 - Gestione della sicurezza secondo codici di comportamento o meccanismi di certificazione

Coerentemente con quanto previsto dall'art. 32 comma 3 del GDPR, l'Istituto ha facoltà di ricorrere a codici di condotta e a schemi di certificazione per dimostrare la conformità ai requisiti di cui all'art. 32 comma 1 del GDPR.

Allorquando i suddetti codici di condotta e/o schemi di certificazione siano stati emessi dal Garante per la protezione dei dati personali ed approvati rispettivamente ai sensi degli artt. 40 e 42 del GDPR, viene data facoltà all'Istituto di aderire ai suddetti codici e schemi, con il coordinamento e la consulenza del Responsabile della protezione dei dati.

Nel caso in cui entro il 31-7-2018 i suddetti codici di condotta e/o meccanismi di certificazione approvati non siano stati ancora emessi dall'Autorità Garante per la protezione dei dati personali, viene data facoltà al Responsabile della protezione dei dati di valutare, proporre e coordinare l'adesione a schemi internazionali di certificazione di sicurezza, al fine di poter dimostrare la conformità ai requisiti dell'art. 32 del GDPR – Sicurezza del trattamento, secondo il principio di responsabilizzazione ("accountability"), e di mettere in atto un SGSI – Sistema per la Gestione della Sicurezza delle Informazioni conforme (ad esempio) ai seguenti standard internazionali di sicurezza:

- ISO / IEC 27001 (norma vera e propria)
- ISO / IEC 27002 (best practice e raccomandazioni in materia di sicurezza)
- Annex-A ("Control Objectives and Controls").

Registro delle Attività di Trattamento, ai sensi dell'art. 30 del Regolamento UE 2016/679

Nome documento:	Registro delle Attività di Trattamento, ai sensi dell'art. 30 del Regolamento UE 2016/679
Codice documento:	IC e IS – Registro Attività Trattamento Ver 1-0
Nome file:	IC e IS – Registro Attività Trattamento Ver 1-0
Stato documento:	Definitivo
Versione:	1.0
Data creazione:	23 maggio 2018
Data ultimo aggiornamento	5 giugno 2018

Indice

Art. 1 - Identificazione e dati di contatto del titolare

Il titolare del trattamento dei dati è l'Istituto nel suo complesso, rappresentato dal Dirigente Scolastico in quanto Legale Rappresentante dell'Ente. I dati di contatto del titolare sono quelli riportati nella prima pagina del presente documento

Art. 2 - Identificazione e dati di contatto del Responsabile della protezione dei dati

Il Responsabile della protezione dei dati designato ai sensi dell'art. 37 del Regolamento UE 2016/679 è il Dott. Giancarlo Favero della ditta Swisstech S.r.l., che può essere contattato alla mail giancarlo.favero@datasecurity.it e al numero 335-5950674.

Art. 3 - Finalità del trattamento: Gestione del Personale Docente

Art. 3.1 - Categorie di interessati e categorie di dati personali

- categorie di interessati: personale docente a tempo determinato ed indeterminato
- dati anagrafici degli insegnanti a tempo indeterminato, insegnanti a tempo determinato, insegnanti esterni incaricati di funzioni nella scuola: nome, cognome, indirizzo, numeri di telefono, di telefax, indirizzo di posta elettronica, ecc.;
- dati dei familiari degli insegnanti a tempo indeterminato, insegnanti a tempo determinato, insegnanti esterni incaricati di funzioni nella scuola;

- dati relativi alle assenze per malattia;
- dati relativi alle assenze per permessi familiari (congedi parentali) e per ragioni di studio/formazione/aggiornamento;
- dati relativi ai permessi per familiari portatori di handicap riconosciuto (Legge 104/92, L. 53/2000);
- dati relativi ai permessi per maternità/paternità;
- dati relativi ai permessi sindacali/amministrativi;
- dati relativi alle ferie;
- dati relativi all'analisi delle situazione di carriera (certificato di servizio e dichiarazione dei servizi prestati);
- contratti di lavoro;
- dati inerenti alla retribuzione/stipendi (dati bancari);
- titoli di studio, dati sul grado di istruzione;
- dati relativi alle altre attività eventualmente svolte dal personale docente;
- comunicazioni al personale necessarie alla gestione amministrativa del rapporto lavorativo (lettere, circolari, avvisi, ecc.);
- dati relativi alla gestione del contenzioso e dei procedimenti disciplinari;
- convocazioni in tribunale;
- dati relativi ai permessi per la donazione del sangue;
- dati relativi ai permessi non retribuiti per i supplenti;
- dati relativi ai permessi previsti dagli artt. 15, 16 DEL CCNL 29/11/07;
- dati necessari per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero della Pubblica Istruzione e dell'ordinamento scolastico;
- dati relativi alla partecipazione a scioperi;
- dati relativi alla partecipazione ad assemblee sindacali.

Art. 3.2 - Natura dei dati

I dati trattati sono di natura comune, sensibile (dati idonei a rivelare le convinzioni religiose, filosofiche, sindacali, d'altro genere; dati idonei a rivelare lo stato di salute, in relazione alle patologie attuali e/o pregresse e alle terapie in corso; dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro; gestione del contenzioso e procedimenti disciplinari; dati idonei a rivelare la vita sessuale, esclusivamente in caso di rettificazione di attribuzione di sesso) e dati di carattere giudiziario (gestione del contenzioso e procedimenti disciplinari).

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

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

I dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali;

I dati idonei sulle convinzioni religiose per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose.

I dati sulle convinzioni religiose vengono in rilievo anche ai fini del reclutamento dei docenti di religione.

I dati sulle convinzioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza;

I dati di carattere giudiziario sono trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l'adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato.

Le informazioni sulla vita sessuale possono desumersi unicamente in caso di eventuale rettificazione di attribuzione di sesso.

Art. 3.3 - Ambito di comunicazione dei dati

- MPI, Ufficio Scolastico Regionale, Ufficio Scolastico Provinciale;
- altri Istituti Scolastici, Enti di formazione;
- Ufficio di collocamento (dati dei supplenti, dati anagrafici, dati sul grado d'istruzione, durata della supplenza);
- Direzione Provinciale dei Servizi Vari (tesoreria),Ragioneria Provinciale dello Stato;
- INPS, INDIRE, Ministero dell'Economia;

- sindacati che con domanda motivata richiedano dati relativi ad attività esclusivamente connessa alle loro funzioni;
- assicurazioni private, INAIL, Revisore contabile, A.S.S.;
- musei, teatri, agenzie di viaggi, fondazioni;
- Comune, Provincia, Regione ed altri Enti Pubblici, anche per il personale assunto obbligatoriamente ai sensi della L. 68/1999;
- Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;
- Organi preposti al riconoscimento della causa di servizio/equo indennizzo» ai sensi del DPR 461/2001;
- Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (d.lg. n. 81/2008)
- Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del DPR. n. 1124/1965;
- Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali
- Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;
- Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge 18 luglio 2003 , n. 186;
- Organi di controllo (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex Legge n. 20/94 e DPR 20 febbraio 1998, n.38;
- Agenzia delle Entrate: ai fini degli obblighi fiscali del personale ex Legge 30 dicembre 1991, n. 413;

- MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335.
- Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art. 50, comma 3, d.lg. n. 165/2001);
- Ministero del Lavoro e delle Politiche Sociali: per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi a Collegi di conciliazione ex D.Lgs. 30 marzo 2001, n. 165;
- Organi arbitrali: per lo svolgimento delle procedure arbitrali ai sensi dei CCNL di settore;
- Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di Giustizia;
- Magistrature ordinarie e amministrative-contabile e Organi di polizia giudiziaria per l'esercizio dell'azione di giustizia;
- Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

Art. 3.4 - Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Art. 3.5 - Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Art. 3.6 - Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS

- invio periodico del modello MMS al Responsabile della protezione dei dati
- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni
- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

Art. 4 - Finalità del trattamento: Gestione degli Alunni

Art. 4.1 - Categorie di interessati e categorie di dati personali

- categorie di interessati: alunni ed ex-alunni
- dati anagrafici degli alunni: nome, cognome, indirizzo, numeri di telefono, di telefax, indirizzo di posta elettronica, ecc.;
- dati personali dei familiari degli alunni;
- dati relativi alle assenze;
- certificati medici;
- valutazione dell'alunno;
- diplomi ed attestati;
- scelta relativa all'ora di religione;
- curriculum scolastico (promozioni, bocciature);
- comunicazioni tra scuola e studente/famiglia dello studente;
- tasse scolastiche (esoneri);
- dati relativi alla gestione del contenzioso;
- dati relativi ad eventuali handicap;
- lettere e comunicazioni alle famiglie;
- fotografie, riprese audio-video (eventuali).

I dati sopra descritti riguardano anche gli ex allievi dell'Istituto: tali dati sono conservati per il periodo previsto dalla legge.

Art. 4.2 - Natura dei dati

I dati trattati sono di natura comune, sensibile (dati idonei a rivelare l'origine razziale o etnica, per favorire l'integrazione degli alunni stranieri; dati idonei a rivelare le 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; dati idonei a rivelare le convinzioni filosofiche, politiche, d'altro genere, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei familiari; dati idonei a rivelare lo stato di salute, in relazione alle patologie attuali e/o pregresse e alle terapie in corso, per assicurare l'erogazione del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate a quelle motorie e sportive, alle visite guidate e ai viaggi d'istruzione, all'erogazione del servizio mensa) e dati a carattere giudiziario (nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno e/o della famiglia dell'alunno, oppure per la gestione del contenzioso con le famiglie degli alunni).

Art. 4.3 - Ambito di comunicazione dei dati

- MPI, Ufficio Scolastico Provinciale, Ufficio Scolastico Regionale;
- assicurazioni private, INAIL, ASS;
- Consolati, direttori centri cultura esteri;
- musei, teatri, agenzie di viaggi, fondazioni;
- Procura della Repubblica, Tribunale dei minori, Tribunale;
- Comune, Provincia, Regione ed altri Enti Pubblici per la fornitura dei servizi ai sensi del D. Lgs. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio;

- S.I.D.D.I.F. - Sistema informativo per il Diritto/Dovere all'Istruzione e alla Formazione (contenente l'Anagrafe degli studenti e l'Osservatorio sulla scolarità);
- ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;
- altri Istituti Scolastici, statali e non, enti di formazione;
- ad aziende, imprese e altri soggetti pubblici e/o privati per tirocini formativi, stages e alternanza scuola-lavoro ai sensi della Legge 24 giugno 1997, n. 196 e del D. Lgs. 21 aprile 2005 n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizi;
- Associazioni Sportive, Professionisti (per specifici progetti);
- Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di Giustizia;
- Magistrature ordinarie e amministrative-contabile e Organi di polizia giudiziaria per l'esercizio dell'azione di giustizia;
- Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

Art. 4.4 - Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Art. 4.5 - Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Art. 4.6 - Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS

- invio periodico del modello MMS al Responsabile della protezione dei dati
- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni
- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

Art. 5 - Finalità del trattamento: Gestione del Personale ATA

Art. 5.1 - Categorie di interessati e categorie di dati personali

- categorie di interessati: personale ATA
- dati anagrafici del personale ATA;
- dati dei familiari del personale ATA;
- dati relativi alle assenze per malattia;
- dati relativi alle assenze per permessi familiari (congedi parentali) e per ragioni di studio/formazione/aggiornamento;
- dati relativi ai permessi per familiari portatori di handicap riconosciuto (Legge 104/92, L. 53/2000);
- dati relativi ai permessi per maternità/paternità;
- dati relativi ai permessi sindacali/amministrativi;
- dati relativi alle ferie;
- dati relativi all'analisi delle situazione di carriera (certificato di servizio e dichiarazione dei servizi prestati);
- contratti di lavoro;
- dati inerenti alla retribuzione/stipendi (dati bancari);
- titoli di studio;
- comunicazioni al personale necessarie alla gestione amministrativa del rapporto lavorativo (lettere, circolari, avvisi, ecc.);
- dati relativi alla gestione del contenzioso e dei procedimenti disciplinari;
- convocazioni in tribunale;
- dati relativi ai permessi per la donazione del sangue;
- dati relativi ai permessi non retribuiti per i supplenti;
- dati relativi ai permessi previsti dagli artt. 15, 16 DEL CCNL 29/11/07;

- dati necessari per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero della Pubblica Istruzione e dell'ordinamento scolastico;
- dati relativi alla partecipazione a scioperi;
- dati relativi alla partecipazione ad assemblee sindacali.

Art. 5.2 - Natura dei dati

I dati trattati sono di natura comune, sensibile (dati idonei a rivelare le convinzioni religiose, filosofiche, sindacali, d'altro genere; dati idonei a rivelare lo stato di salute, in relazione alle patologie attuali e/o pregresse e alle terapie in corso; dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro; gestione del contenzioso e procedimenti disciplinari; dati idonei a rivelare la vita sessuale, esclusivamente in caso di rettificazione di attribuzione di sesso) e dati di carattere giudiziario (gestione del contenzioso e procedimenti disciplinari).

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

I dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali;

I dati idonei sulle convinzioni religiose per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose.

I dati sulle convinzioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza;

I dati di carattere giudiziario sono trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l'adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato.

Le informazioni sulla vita sessuale possono desumersi unicamente in caso di eventuale rettificazione di attribuzione di sesso.

Art. 5.3 - Ambito di comunicazione dei dati

- MPI, Ufficio Scolastico Regionale, Ufficio Scolastico Provinciale;
- altri Istituti Scolastici, Università, Enti di formazione;
- Direzione Provinciale dei Servizi Vari (tesoreria), Ragioneria Provinciale dello Stato;
- INPS, INDIRE, Ministero dell'Economia;
- sindacati che con domanda motivata richiedano dati relativi ad attività esclusivamente connessa alle loro funzioni;
- assicurazioni private, INAIL, Revisore contabile, ASL;

- musei, teatri, agenzie di viaggi, fondazioni;
- Procura della Repubblica;
- Comune, Provincia, Regione ed altri Enti Pubblici, anche per il personale assunto obbligatoriamente ai sensi della L. 68/1999;
- Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;
- Organi preposti al riconoscimento della causa di servizio/equo indennizzo» ai sensi del DPR 461/2001;
- Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (D.lg. n. 81/2008);
- Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del DPR. n. 1124/1965;
- Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;
- Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;
- Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge 18 luglio 2003, n. 186;
- Ufficio di collocamento (dati dei supplenti, dati anagrafici, dati sul grado d'istruzione, durata della supplenza);
- Organi di controllo (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex L. n. 20/94 e DPR 20 febbraio 1998, n. 38;
- Agenzia delle Entrate: ai fini degli obblighi fiscali del personale ex Legge 30 dicembre 1991, n. 413;

- MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335;
- Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e finzioni pubbliche elettive (art. 50, comma 3, d.lg. n. 165/2001);
- Ministero del Lavoro e delle Politiche Sociali: per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi a Collegi di conciliazione ex D.Lgs. 30 marzo 2001, n. 165;
- Organi arbitrali: per lo svolgimento delle procedure arbitrali ai sensi dei CCNL di settore;
- Avvocature dello Stato: per la difesa erariale e consulenza presso gli organi di Giustizia;
- Magistrature ordinarie e amministrative-contabile e Organi di polizia giudiziaria per l'esercizio dell'azione di giustizia;
- Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

Art. 5.4 - Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Art. 5.5 - Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Art. 5.6 - Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS

- invio periodico del modello MMS al Responsabile della protezione dei dati
- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni
- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

Art. 6 - Finalità del trattamento: Gestione Alunni Diversamente Abili (Alunni "H")

Art. 6.1 - Categorie di interessati e categorie di dati personali

Relativamente ad alunni portatori di handicap, l'Istituto tratta anche i seguenti dati:

- documentazione e lettere relative all'alunno;
- PEI Piano educativo individualizzato (si fa riferimento alla diagnosi);
- PDF profilo dinamico funzionale (si fa riferimento alla diagnosi);
- comunicazioni con famiglia e operatori sanitari;
- relazione finale;
- "certificazione" analisi mediche relativi all'Handicap;
- "diagnosi funzionale";
- valutazioni e verbali dell'alunno;
- accertamento Commissione Sanitaria ex DPCM 23/02/2006 n. 185;
- lettere e corrispondenza riservata con medici, Istituti specialistici.

Art. 6.2 - Natura dei dati

I dati trattati sono di natura comune e sensibile.

Art. 6.3 - Ambito di comunicazione dei dati

- Professionisti, strutture ospedaliere;
- ASS e Enti Locali per il funzionamento dei Gruppi di Lavoro di istituto per l'Handicap e per la predisposizione e la verifica del Piano Educativo Individuale ai sensi della Legge 5 febbraio 1992, n. 104;
- Cooperative private di sostegno agli allievi "H";
- Enti Pubblici.

Art. 6.4 - Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Art. 6.5 - Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Art. 6.6 - Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS
- invio periodico del modello MMS al Responsabile della protezione dei dati
- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni

- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati
- in caso di trattamento di dati sensibili o giudiziari, ottemperanza a quanto prescritto dal Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007), ai sensi dell'art 6 comma 2 del Regolamento UE 2016/679.

Art. 7 - Finalità del trattamento: Gestione Fornitori di Beni e Servizi

Art. 7.1 - Categorie di interessati e categorie di dati personali

- dati anagrafici fornitori: nome, cognome, codice fiscale, indirizzo, P.IVA, denominazione/ragione sociale, sede legale/amministrativa, coordinate bancarie, referenti interni, telefono, indirizzo e-mail, ecc;
- documenti contabili/fiscali;
- preventivi, offerte;
- comunicazioni tra Istituto e fornitori;
- contratti e convenzioni.
- lettere e corrispondenza riservata con medici, Istituti specialistici.

Art. 7.2 - Natura dei dati

I dati trattati sono di natura comune.

Art. 7.3 - Ambito di comunicazione dei dati

- Ufficio Scolastico Provinciale, MPI, Ministero delle Finanze;
- altri istituti scolastici;
- Direzione provinciale dei Servizi Vari (Tesoreria);
- Comune, Provincia, Regione ed altri Enti Pubblici;
- Revisore dei conti;
- Fondazioni, Istituti Bancari, Assicurazioni;
- Professionisti: (Studi legali, Arbitri, ecc.).

Art. 7.4 - Trasferimenti di dati verso un paese terzo

I dati non sono trasferiti verso un paese terzo o verso un'organizzazione internazionale, fatta eccezione per i casi in cui i dati siano gestiti in cloud ed i server siano fisicamente collocati all'estero. In ogni caso i server sono fisicamente ubicati in un paese appartenente all'Unione Europea.

Art. 7.5 - Termini previsti per la cancellazione delle diverse categorie di dati

I dati sono di norma conservati per un periodo non superiore a quello necessario al conseguimento delle finalità per la quali sono stati raccolti, e in ottemperanza a quanto prescritto dalla Soprintendenza Archivistica Regionale.

Art. 7.6 - Misure tecniche ed organizzative di sicurezza di cui all'art. 32 del Regolamento UE 2016/679

- autenticazione informatica
- adozione di procedure di gestione delle credenziali di autenticazione
- credenziali di autenticazione attribuite e utilizzate su base nominativa individuale
- utilizzazione di un sistema di autorizzazione
- utilizzazione di un sistema di profilazione
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
- disattivazione degli account non più utilizzati
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici

- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- designazione del Responsabile della protezione dei dati
- individuazione degli eventi che possono compromettere la sicurezza
- compilazione periodica del modello MMS
- invio periodico del modello MMS al Responsabile della protezione dei dati
- verifiche periodiche da parte del Responsabile della protezione dei dati
- adozione di schemi di certificazione relativamente all'impostazione ed alla gestione di un modello per la gestione della privacy e della sicurezza delle informazioni
- tenuta del registro delle violazioni dei dati
- adozione di una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative
- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti
- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Allegato: Decreto del Ministero della Pubblica Istruzione 7 dicembre 2006, n. 305, recante il Regolamento per il trattamento dei dati sensibili e giudiziari in ambito scolastico (G.U. n. 11 del 15 gennaio 2007)

Istituto Comprensivo di Traona
Costiera dei Cech

Ministero dell'Istruzione, dell'Università e della Ricerca
ISTITUTO COMPRENSIVO DI TRAONA
Via Aldo Moro n. 6 - 23019 TRAONA (SO) - Tel. 0342 653340
Codice Fiscale: 82003850144 - Codice Ufficio Univoco UFZVHU
e-mail: SOIC81200L@ISTRUZIONE.IT - SOIC81200L@PEC.ISTRUZIONE.IT
sito web: www.ictraona.it

PON 2014-2020
Unione Europea

REGISTRO DEGLI INCIDENTI INFORMATICI E DELLE VIOLAZIONI DI DATI (ARTT. 33 E 34 DEL GDPR) Dati di contatto del Responsabile della protezione dei dati: Dott. Giancarlo Favero, Cell. 335-5950674, mail: giancarlo.favero@datasecurity.it

La violazione dei dati deve essere tempestivamente notificata al Responsabile della protezione dei dati

Data Violazione	Tipologia violazione	Sistema impattato	Tipi di dati coinvolti	Data notificazione a Data Protection Officer	Data notificazione a Garante per la protezione dei dati	Rif. Scheda Violazione Dati