ITET
SALVEMINI

REGOLAMENTO

PER LA PROTEZIONE DEI DATI

A.S. 2016/2017

Data stesura:	Approvato da:	in qualità di:	firma
24/03/2017	Dirigente Scolastico	Titolare trattamento dati	
	Consiglio di Istituto	Organo competente	

Data revisioni:	Approvato da:	in qualità di:	firma

ITET
SALVEMINI

INDICE

Sommario

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it

1 Campo di applicazione

Il presente documento si applica al trattamento dei dati personali raccolti nell'ambito delle finalità istitutive dell'attività svolta dal titolare del trattamento.
La normativa alla quale si fa riferimento è la seguente: Decreto legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali.
In questo regolamento vengono definiti i criteri tecnici e organizzativi per garantire la sicurezza dei dati personali trattati dall'Istituto come di seguito illustrati:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento dei dati o degli strumenti elettronici;
- la previsione degli interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Nella redazione del presente documento si sono tenuti presente i seguenti obiettivi:

- avere una visione la più possibile completa e dettagliata del grado di esposizione a varie tipologie di rischi cartacei e informatici;
- individuare e mettere in atto non solo le misure minime di sicurezza prescritte dal Codice e dal Disciplinare tecnico, ma, dove possibile, le misure idonee (organizzative, tecnologiche, logistiche, normative e procedurali) atte a garantire la protezione dei dati personali;
- assicurare che la gestione dei dati personali e più in generale di tutti i dati necessari all'attività dell'Istituto avvenga con un ragionevole livello di sicurezza e riservatezza nel corso di tutte le modalità di trattamento, comprese quelle che utilizzano strumenti diversi da quelli elettronici.

Il Codice prescrive inoltre che i dati personali oggetto di trattamento siano custoditi e controllati anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non

autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31 – Obblighi di sicurezza).
A questo scopo sono indicate una serie di misure minime di sicurezza già adottate o in corso di realizzazione che riguardano i trattamenti effettuati con strumenti elettronici:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- 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;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari

2 Descrizione dei trattamenti

2.1 Tipologia dei dati

Definizioni riportate dall'art. 4 del Codice:
"trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
"dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
"dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
*"**dati giudiziari**"*, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

2.2 Indicazioni del trattamento

Identificazione dei tipi di dati sensibili e giudiziari e delle operazioni su questi eseguibili.
(MINISTERO DELLA ISTRUZIONE - DECRETO 7 dicembre 2006, n.305)
Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali».

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it

SCHEDA 1:
Selezione e reclutamento a Tempo Indeterminato e Determinato, e Gestione Del Rapporto

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, protezione della maternità, igiene e sicurezza sul luogo di lavoro, causa di servizio, svolgimento di pratiche assicurative, pensionistiche e previdenziali obbligatori e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortuni/sinistri e malattie professionali, fruizione di assenze e permessi lavorativi, per il personale particolari condizioni di salute dell'interessato o dei suoi familiari, assistenza fiscale, mobilità territoriale, professionale e intercompartimentale;
DATI IDONEI A RILEVARE L'ADESIONE A SINDACATI o ad organizzazioni sindacali, per gli adempimenti connessi al versamento delle quote di iscrizione ed all'esercizio dei diritti sindacali;
DATI SULLE CONVINZIONI RELIGIOSE per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato, motivata per ragioni di appartenenza a determinate confessioni religiose. I dati sulle convinzioni religiose vengono in rilievo anche ai fini del reclutamento dei docenti di religione;
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;
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.

SCHEDA 2:
Gestione del contenzioso e procedimenti disciplinari
Il trattamento dei dati sensibili e giudiziari concerne tutte le attività relative alla difesa in giudizio del Ministero dell'Istruzione e delle Istituzioni scolastiche nel contenzioso del lavoro amministrativo nonché connesse alla gestione degli affari penali e civili.

SCHEDA 3:
Organismi collegiali e commissioni istituzionali
Il trattamento dei dati sensibili è necessario per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero Istruzione e dell'ordinamento scolastico. Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, delle famiglie e delle associazioni sindacali. Il dato sensibile trattato è quello dell'appartenenza alle organizzazioni sindacali, con riferimento agli organismi o comitati che richiedano la partecipazione di rappresentati delle organizzazioni sindacali.

SCHEDA 4:
Attività propedeutiche all'avvio dell'anno scolastico
I dati sono forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio nelle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.
Nell'espletamento delle attività propedeutiche all'avvio dell'anno scolastico da parte delle istituzioni

scolastiche, possono essere trattati dati sensibili relativi:

- alle origini razziali ed etniche, per favorire l'integrazione degli alunni con cittadinanza non italiana;
- alle convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento;
- allo stato di salute, per assicurare l'erogazione del sostegno agli alunni diversamente abili e per la composizione delle classi;
- alle vicende giudiziarie, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione.

I dati giudiziari emergono anche nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno nonché nei confronti degli alunni che abbiano commesso reati.

SCHEDA 5:
Attività educativa, didattica e formativa, di valutazione
Nell'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami, da parte delle istituzioni scolastiche di ogni ordine e grado, ìvi compresi convitti, educandati e scuole speciali, possono essere trattati dati sensibili relativi:

- alle origini razziali ed etniche per favorire l'integrazione degli alunni con cittadinanza non italiana;
- alle convinzioni religiose per garantire la libertà di credo religioso;
- allo stato di salute, per assicurare l'erogazione del servizio di refezione scolastica, del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate e ai viaggi di istruzione;
- ai dati giudiziari, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione;
- alle convinzioni politiche, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei genitori.

I dati sensibili possono essere trattati per le attività di valutazione periodica e finale, per le attività di orientamento e per la compilazione della certificazione delle competenze.

SCHEDA 6:
Rapporti scuola-famiglie: gestione del contenzioso
Il trattamento di dati sensibili e giudiziari concerne tutte le attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, etc.) con gli alunni e con le famiglie, e tutte le attività relative alla difesa in giuridico delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.

2.3 Finalità del trattamento

Il trattamento dei dati personali è funzionale al raggiungimento delle finalità di istruzione e di formazione in ambito scolastico, professionale e superiore, con particolare riferimento a quelle svolte anche in forma integrata, ed è quindi di rilevante interesse pubblico, ai sensi degli articoli 20 e 21 del

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it

D.lgs 196/2003. Per le sue finalità istituzionali, l'Istituzione scolastica tratta dati personali, sia comuni che sensibili o giudiziari, di studenti, genitori, personale dipendente e fornitori.

2.4 Elenco dei trattamenti

Nella tabella riportata nel presente paragrafo viene mostrato, a seguito della verifica eseguita, l'elenco dei trattamenti dei dati rilevanti ai sensi del D.LGS 196/03 e del Regolamento adottato dal Ministero, secondo le seguenti specifiche:

- **Identificativo del trattamento**: consiste in un codice, facoltativo, ma utile per il titolare, in quanto consente un'identificazione univoca e più rapida di ciascun trattamento nella compilazione delle altre tabelle
- **Descrizione sintetica**: descrive il trattamento in modo da consentire una comprensione immediata della tabella.
- **Natura dei dati trattati:** viene indicato se, tra i dati oggetto del singolo trattamento elencato, sono presenti dati sensibili o giudiziari, oltre ad altri dati personali.
- **Area di riferimento**: indica la struttura (o reparto, funzione, ufficio, ecc.) all'interno della quale viene realizzato il trattamento.
- **Finalità di rilevante interesse pubblico** descritte nelle schede allegate al decreto 305/2006.
- **Altre funzioni che concorrono al trattamento***:* nel caso in cui un trattamento, per essere completato, comporti l'attività di diverse strutture vengono indicate oltre quella che primariamente detiene la responsabilità dell'attività, anche quelle che concorrono, siano esse interne od esterne all'organizzazione del titolare.

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it

ID	Descrizione sintetica del trattamento			Natura dei dati			Struttura di riferimento	Descrizione degli strumenti utilizzati
	Finalità perseguita o att. svolta	Categorie di interessati	Terzi a cui vengono comunicati i dati	N	S	G	altre strutture che concorrono al trattam.	
T1	**Alunni** Attività didattica	**- Alunni** **- Genitori**	UST, USR, MIUR, Altre istituzioni scolastiche, Invalsi, ASL, Enti Locali, gestori pubblici e privati dei servizi di assistenza, Istituti di assicurazione, INAIL.	X	X	X	**Dirigente** **Docenti** Componenti org.smi collegiali e comm.ni istituzionali Collaboratori del DS Responsabili trattamento esterni Segreteria Coll. Scolastici	**Documenti** formato cartaceo formato elettronico
T2	**Alunni** Fasi propedeutiche avvio anno scolastico	**- Alunni** **- Genitori**	Aziende, Imprese altri soggetti pubblici o privati per tirocini formativi, stage e alternanza scuola lavoro. Avvocatura dello Stato Magistratura ordinaria, amministrativa contabile. Organi di polizia giudiziaria, Liberi professionisti.	X	X	X	**Dirigente** **Segreteria** Collaboratori del DS Docenti Responsabili trattamento esterni Componenti org.smi collegiali e comm.ni istituzionali Coll. Scolastici	**Documenti** formato cartaceo formato elettronico

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it

T3	**Personale dipendente** Selezione e reclutamento a tempo indeterminato e determinato del rapporto di lavoro del personale	**- Personale**	UST, USR, MIUR, altre Istituzioni Scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, ASL, Altre Amm. Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali, assicurativi. Organi preposti alla vigilanza su igiene e sicurezza. Agenzia delle Entrate. Organi preposti agli accert. per idoneità impiego.	X	X	X	**Dirigente Segreteria** Collaboratori del DS Responsabili trattamento esterni Componenti org.smi collegiali e comm.ni istituzionali	**Documenti** formato cartaceo formato elettronico
T4	**Collabor.ri professionali** Incarichi Contratti di prestazione d' opera per attività d' Istituto	**- Personale interno** **- Personale esterno**	Agenzia delle Entrate, Ragioneria Territoriale dello Stato, INPS, INPDAP, Altre Amministrazioni Pubbliche	X			**Dirigente Segreteria** Collaboratori del DS Responsabili trattamento esterni Componenti org.smi collegiali e comm.ni istituzionali	**Documenti** formato cartaceo formato elettronico

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it

T5	**Acquisti e fornitori** Acquisto di servizi e materiale	**- Fornitori**	Banca che effettua il servizio di cassa	X			**Dirigente Segreteria** Collaboratori del DS Responsabili trattamento esterni Componenti org.smi collegiali e comm.ni istituzionali	**Documenti** formato cartaceo formato elettronico
T6	**Gestione finanziaria e del bilancio** Atti di gestione finanziaria, contabile, patrimoniale	**Personale** **Fornitori**	UST, USR, MIUR, Agenzia delle Entrate, Altre Istituti Scolastici, NPDAP, INPS, INAIL, ASL, Altre Amm.ni Pubbliche, Corte dei Conti, MEF, Banca che effettua il servizio di cassa	X			**Dirigente Segreteria** Collaboratori del DS Responsabili trattamento esterni Componenti org.smi collegiali e comm.ni istituzionali	**Documenti** formato cartaceo formato elettronico

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it

T7	**Gestione Istituzionale e Protocollo** Comunicazioni da e per Enti Esterni Comunicaz. interna	**Alunni, Genitori Fornitori Personale interno Personale esterno Personale Altre Amm.ni**	UST, USR, MIUR, Altre Istituzioni Scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, AUSL, Altre PA, Corte dei Conti, MEF, Enti assistenziali, previdenziali E assicurativi. Organi preposti alla vigilanza su igiene e sicurezza. Agenzia delle Entrate, Organi preposti agli accertamenti, idoneità impiego. Banca che effettua il servizio di cassa	X	X	X	**Dirigente Segreteria** Collaboratori del DS Responsabili trattamento esterni Componenti org.smi collegiali e comm.ni istituzionali	**Documenti** formato cartaceo formato elettronico
T8	**Trattamenti da parte di persone, anche esterne alla scuola, facenti parte degli organi collegiali**	**Alunni, Personale Utenti del Servizio Scolastico, ecc.**	Rapporti istituzionali con enti e privati	X	X		**Dirigente Segreteria** Componenti org.smi collegiali e comm.ni istituzionali Collaboratori del DS Responsabili trattamento esterni Coll. Scolastici	**Documenti** formato cartaceo formato elettronico
T9	**Trattamenti di dati effettuati da Collaboratori Scolastici e Personale Ausiliario**	**Alunni, genitori, personale**	Comune	X	X		**Collaboratori Scolastici Segreteria Dirigente Scolastico**	supporto a tutti i trattamenti

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it

LEGENDA:

N= dati non sensibili e non giudiziari S= sensibili G= giudiziari

T1 - Alunni - Dati personali trattati da Docenti
T2 - Alunni – Dati personali trattati da Assistenti Amministrativi e DSGA
T3 - Personale dipendente -– Dati personali trattati da Assistenti Amministrativi e Tecnici e DSGA
T4 - Collaborazioni professionali -– Dati personali trattati da Assistenti Amministrativi e DSGA
T5 - Acquisti e fornitori - Dati personali trattati da Assistenti Amministrativi e DSGA
T6 - Gestione finanziaria e del bilancio-– Dati personali trattati da Assistenti Amministrativi e DSGA
T7 - Gestione Istituzionale e Protocollo-– Dati personali trattati da Assistenti Amministrativi e DSGA
T8 - Gestione di trattamenti da parte di persone, anche esterne alla scuola, facenti parte degli organi collegiali
T9 – Trattamenti di dati personali effettuati da Collaboratori Scolastici e Personale Ausiliario

Dettaglio dei dati suddiviso per tipologia, modalità di raccolta dei dati e di trattamento, archivi cartacei/o elettronici utilizzati, elenco dei principali dati comunicati ad enti pubblici o privati esterni alla scuola.

Nella stesura del presente documento si dovrà tener conto della seguente legenda:
"T + numero" indica la categoria generale
"C + suffisso" indica trattamenti **Cartacei**, il suffisso "S" indica dati sensibili, il suffisso "SG" indica dati sensibili e giudiziari, "N" dati non sensibili e non giudiziari
"E + suffisso" indica trattamenti con **Elaboratore** elettronico, il suffisso "S" indica dati sensibili, il suffisso "SG" indica dati sensibili e giudiziari, "N" dati non sensibili e non giudiziari.
"T + suffisso", indica comunicazioni **Telematiche**, il suffisso "S" indica dati sensibili, il suffisso "SG" indica dati sensibili e giudiziari, "N" dati non sensibili e non giudiziari.

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it

3 Compiti e responsabilità

3.1 Titolare del trattamento e obblighi

Il Titolare del trattamento dei dati è identificato nella figura del Dirigente Scolastico, **Prof. Donato Ferrara**, quale rappresentante dell'Istituto.

Al titolare competono le decisioni in ordine alle finalità ed alle modalità del trattamento dei dati personali, ivi compreso il profilo della sicurezza.
Il titolare del trattamento dei dati oggetto di questo documento è esonerato dalla "notificazione al Garante" poiché non esegue alcune tipologia di trattamento specificato nell'art. 37 del Codice sulla Privacy, verificato anche alla luce delle chiarificazioni fornite dal garante il 23 marzo 2004 ed il 16 aprile 2004. Si fa riferimento alla autorizzazione n. 1/2000 al trattamento dei dati sensibili nei rapporti di lavoro, pubblicata sulla GU n. 229 del 30/09/2000. Tali autorizzazioni sono rinnovate nel 2002.
Il titolare è obbligato ad informare la persona cui si riferiscono i dati personali raccolti, in relazione ai diritti riconosciuti.

3.2 Responsabile del trattamento

Il Responsabile del trattamento dei dati è identificato nella figura del D.S.G.A. **dott.ssa Emilia Binetti**
Il Responsabile del trattamento dei dati è equiparato come poteri al titolare del trattamento con il quale condivide le responsabilità e le relative conseguenze civili, penali ed amministrative in caso di inadempienze. Viene individuato in relazione all'esperienza, capacità ed affidabilità, dal titolare, e procede al trattamento dei dati attenendosi alle istruzioni impartite per mezzo del presente documento.
Egli da istruzioni agli incaricati del trattamento e vigila sulla puntuale osservanza delle disposizioni, anche tramite verifiche periodiche.
Inoltre, egli dovrà adottare tutte le misure delle quali si renda necessaria l'adozione immediata ed urgente, al fine di procedere alla tutela dei dati.
Il responsabile segnalerà:

- eventuali reclami da parte degli interessati (personale della scuola, genitori, etc.)
- qualunque fatto che a suo giudizio possa compromettere la sicurezza dei dati

Egli revisiona annualmente il presente documento di programmazione, tenendo conto:

- dei controlli interni sull'efficacia delle misure
- dell'aggiornamento tecnologico dei mezzi idonei ad assicurare la sicurezza dei dati
- delle misure minime dettate dall'aggiornamento legislativo.

3.2.1 Istruzioni impartite dal Titolare al Responsabile del trattamento

1. Rispettare le misure minime di sicurezza previste dalla normativa vigente sulla tutela dei dati personali e disporre gli interventi necessari ad assicurare un livello minimo di protezione dei dati personali, al fine di:

- o ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati trattati;
- o evitare l'accesso non autorizzato ai dati trattati;
- o prevenire trattamenti non conformi alla legge.

2. Individuare e comunicare al dirigente i nominativi oppure le categorie o specifici profili di operatori incaricati del trattamento dei dati.

3. Procedere – ove necessario – al rilascio ed alla revoca delle autorizzazioni previste dagli artt. 12, 13 e 14 del Disciplinare Tecnico in materia di misure minime di sicurezza contenuto all'Allegato B) del D.Lgs. 196/2003, e verificare che l'accesso ai dati da parte degli incaricati sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate.

4. In merito al mantenimento delle autorizzazioni di cui al precedente punto 3, verificare – almeno una volta all'anno – la sussistenza delle condizioni che hanno determinato la loro emissione e, in caso di difetto, procedere alla loro revoca.

5. Comunicare tempestivamente all'Amministratore di Sistema ogni atto ed evento che comporti una disattivazione immediata o modifica dei profili e delle autorizzazioni di accesso alle banche dati e ai programmi applicativi, come ad esempio: dimissioni, assunzioni, trasferimenti da/verso altre Aree/Servizi, cessazione, sospensione o revoca di incarico, variazioni di ruolo/responsabilità, etc.

6. Fornire agli incaricati, le istruzioni per il corretto trattamento dei dati personali ed eseguire gli opportuni controlli.

7. Controllare la pertinenza, non eccedenza e completezza dei dati rispetto alle finalità dei trattamenti di propria competenza.

8. Stabilire le modalità di gestione e le forme di responsabilità relative a banche dati condivise da più unità organizzative, d'intesa con gli altri responsabili.

9. Informare prontamente il Titolare di ogni questione rilevante ai fini di legge.

10. Rispondere tempestivamente all'interessato che richieda di conoscere informazioni relative all'attività di trattamento, ai sensi dell'art. 7 del D.Lgs 196/2003 e successive modifiche ed integrazioni.

11. Rispondere ai reclami degli interessati.

12. Collaborare con il Garante per la protezione dei dati personali nel caso di richiesta di informazioni o di verifiche sui luoghi.

3.3 Incaricato del trattamento

Gli incaricati del trattamento dei dati sono stati identificati per l'Area Docenti e per l'Area Personale ATA**.**

Nel primo caso sono stati incaricati tutti i docenti in servizio. Nel secondo caso sono stati incaricati tutti gli assistenti amministrativi.

Le responsabilità attinenti la gestione dei dati per le diverse tipologie di addetti all'interno del nostro istituto sono individuate e descritte nelle lettere di incarico. L'incaricato del trattamento dei dati è obbligato ad uniformarsi a quanto contenuto nel presente documento ed opera sotto la diretta autorità del titolare o del responsabile. Egli ha accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati. Se all'incaricato vengono affidati documenti cartacei, questi devono essere responsabilmente conservati e restituiti al termine delle operazioni affidate

3.3.1 Istruzioni impartite dal Responsabile agli incaricati del trattamento

1) Il trattamento deve svolgersi in modo lecito e secondo correttezza: i dati personali devono essere raccolti, registrati e trattati esclusivamente per le finalità inerenti l'attività svolta da ciascuno, indicate nella lettera di nomina in conformità a quanto prescritto dal Decreto n. 305/2006 sul regolamento dei dati sensibili e giudiziari adottati dal Ministero della Istruzione;

2) è compito di ciascun incaricato verificare l'esattezza ed il grado di aggiornamento dei dati trattati; che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare o dal Responsabile;

3) i dati devono essere conservati rispettando le misure di sicurezza previste dalla normativa vigente nonché quelle predisposte dall'Istituzione Scolastica garantendo la massima riservatezza in ogni operazione di trattamento e, in particolare, ciascun incaricato dovrà:

a. per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;

b. conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;

c. con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, riporre gli stessi al termine delle operazioni affidate nei luoghi ad accesso controllato predisposti dall'istituzione scolastica;

d. le copie di dati personali su supporti rimovibili sono permesse solo se costituiscono operazione del trattamento approvata dal responsabile. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono essere mai lasciati incustoditi;

e. in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Responsabile del trattamento;

4) ciascun incaricato dovrà segnalare al titolare o al responsabile eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta;

5) nessun dato potrà essere comunicato a terzi o diffuso senza la preventiva specifica autorizzazione del Responsabile del trattamento;

6) la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico deve essere mantenuta per tutta la durata del medesimo e anche successivamente al termine stesso;

3.3.2 Incaricati con responsabilità interne: amministratore di sistema

E' stato identificato come amministratore di sistema il prof. Mauro Ciccolella.

La figura dell' Amministratore di sistema ha il compito di sovrintendere alle risorse del sistema operativo degli elaboratori ed alle dotazioni necessarie all'adeguata conservazione dei dati in modo da consentirne la corretta rintracciabilità ed utilizzazione in ottemperanza alla vigente normativa.

Egli agisce secondo le direttive impartitegli dal titolare o dal responsabile. All'amministratore spetta il rispetto delle disposizioni eventualmente impartite dal Ministero.
Si ritiene necessario individuare tale figura ed eventualmente di distribuire su più incaricati, i compiti e le incombenze procedurali resi obbligatori dalle nuove misure minime di sicurezza previste dal Disciplinare Tecnico.
Per il ruolo ricoperto all'interno dell'organizzazione scolastica e per le competenze tecniche, a tali figure si richiede anche un supporto attivo nel coadiuvare il proprio responsabile e il titolare nell'individuazione di puntuali istruzioni operative attinenti all'applicazione delle misure di sicurezza per il trattamento dei dati personali compiute attraverso strumenti elettronici, a specificazione e chiarimento di quelle generali impartite dai singoli responsabili, nonché il coordinamento dei relativi adempimenti riguardanti le procedure di autenticazione e autorizzazione, assieme all'assistenza in questo campo ai responsabili e agli incaricati del trattamento.

Alcune delle particolarità che caratterizzano l'Amministratore di Sistema sono:

- gestione dei codici e delle password di accesso per la configurazione degli apparati attivi per la trasmissione dei dati sulla rete, dei codici e delle password di accesso per la configurazione del server e l'accesso alle funzioni sistemistiche di manutenzione degli stessi;
- è abilitato al rilascio dei codici e delle password da assegnarsi alle eventuali terze parti da abilitarsi al collegamento al sistema informatizzato della scuola dall'esterno (ad esempio, i fornitori di procedure informatiche ai fini di consentire l'erogazione dell'assistenza da remoto);
- è incaricato di garantire l'efficienza e la disponibilità della rete, dei sistemi informativi e della piattaforma di autenticazione;
- è incaricato di svolgere controlli atti a rilevare eventuali accessi non autorizzati alla rete e ai sistemi;
- è incaricato di mantenere aggiornata la documentazione tecnica relativa alla configurazione hardware e software della rete e degli strumenti di sicurezza;
- è incaricato di garantire l'effettuazione delle operazioni di salvataggio dei database presenti sui server, la non accessibilità di tali copie da parte di terzi non autorizzati, l'efficacia delle procedure di ripristino in caso di danneggiamento dei dati, la distruzione delle copie non più necessarie per le finalità di ripristino;

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it

- è incaricato di assegnare a ciascun incaricato del trattamento il profilo di utenza corrispondente alle sole funzionalità necessarie alla attività istituzionale svolta dal medesimo, concordata con il responsabile del singolo trattamento;

- è incaricato di vigilare, assieme ai responsabili, che i codici per l'identificazione non siano assegnati ad altri incaricati, neppure in tempi diversi;
- è incaricato di garantire la disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi (esclude quelle preventivamente autorizzate per soli scopi di gestione tecnica) e, di concerto con i responsabili, di disattivare le credenziali di autenticazione in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
- è incaricato di garantire gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti.

4 Analisi dei rischi che incombono sui dati

Mediante l'analisi dei rischi che incombono sui dati trattati con strumenti informatici o su supporto cartaceo, è stata eseguita un'analisi per individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutarne le possibili conseguenze e la gravità, per poter porli in correlazione con misure di sicurezza previste dall'Istituto.
L'accertamento dell'integrità dei dati ha riguardato la protezione dei dati stessi dai rischi di possibili modifiche o distruzione, accidentali o deliberate, classificati in:
1) rischi ambientali;
2) rischi specifici per trattamenti con strumenti elettronici;
3) rischi specifici per trattamenti senza l'ausilio di strumenti elettronici.

4.1.1 Rischi ambientali

I rischi ambientali costituiscono la componente più classica dei rischi, quella che riguarda la sicurezza dei locali e degli strumenti che ospitano i dati.
In particolare si è tenuto conto di quali rischi rappresentano una reale minaccia per le strutture che ospitano i dati, valutando specifiche misure di sicurezza da adottare per la protezione degli archivi e sale server. L'accertamento ha evidenziato che i rischi possibili sono legati ad eventi come:

- incendio
- allagamento
- atti di vandalismo

4.1.2 Rischi specifici per trattamenti con strumenti elettronici

L'accertamento dell'integrità e della disponibilità dei dati ha riguardato la protezione dei dati stessi dai rischi di possibili modifiche o distruzione accidentali o deliberate o il fatto che le informazioni non siano disponibili a causa di eventi come:

- sovrascrittura o distruzione dei dati, involontarie ma imputabili ad azioni umane errate;
- sovrascrittura o distruzione dei dati dovute a guasti delle apparecchiature dedicate alla memorizzazione;
- alterazioni dei dati conseguenti ad una teorica azione deliberatamente perpetrata allo scopo di modificare volontariamente i dati, inserire nuovi dati o distruggere i dati;

- alterazioni, distruzione o indisponibilità dei dati connessi alla diffusione dei virus e dei programmi pericolosi, provocata da corruzione dei file eseguibili, corruzione dei dati stessi, corruzione di documenti,

- perdita di file, perdita di spazio utilizzabile nelle memorie, cattivi funzionamenti del sistema, degrado delle prestazioni del sistema, impossibilità di utilizzo del sistema;
- distruzione o alterazione dei dati dovuta a deterioramento nel tempo dei supporti di memorizzazione e del mezzo fisico che li ospita;
- danneggiamento o manomissione delle attrezzature e/o delle connessioni;
- indisponibilità dei dati dovuta ad anomalie in programmi che avrebbero dovuto elaborare i dati e che non hanno potuto completare la loro esecuzione;
- indisponibilità dei dati malfunzionamento hardware (guasti alle unità di elaborazione, di memorizzazione di trasmissione);
- indisponibilità dei dati per dimensionamento non sufficiente delle risorse tecnologiche deputate alla trasmissione ed alla memorizzazione.

4.1.3 Rischi specifici per trattamenti senza l'ausilio di strumenti elettronici

L'accertamento dell'integrità e della disponibilità dei dati ha riguardato la protezione dei dati stessi dai rischi di possibili modifiche o distruzione accidentali o deliberate o il fatto che le informazioni non siano disponibili a causa di eventi come:

- furto, danneggiamento o distruzione dei supporti cartacei sui quali sono conservati i dati;
- mancanza di procedure adeguate di archiviazione che consentano la disponibilità e la reperibilità dei dati.

4.1.4 Tabella riassuntiva dell'analisi dei rischi

I suddetti rischi sono stati ripartiti in classi di gravità, tenendo conto della concreta possibilità di realizzazione presso l'istituzione scolastica, adottando la seguente scansione:
A= alto M = medio B = basso

La tabella seguente sintetizza i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutandone le possibili conseguenze e stimandone la gravità, ponendoli altresì in correlazione con le misure di sicurezza previste.

EVENTO		IMPATTO SULLA SICUREZZA DEI DATI		RIF. MISURE DI AZIONE
		DESCRIZIONE	GRAVITÀ STIMATA	
AZIONI FRAUDOLENTE O ERRORI	Furto di credenziali di autenticazione	Accesso non autorizzato	M	Vigilanza sul rispetto delle istruzioni impartite
	Carenza di consapevolezza, disattenzione o incuria	Dispersione, perdita e accesso altrui non autorizzato	M	Formazione e flusso continuo di informazione
	Comportamenti sleali o fraudolenti	Dispersione, perdita e accesso altrui non autorizzato	M	Vigilanza sul rispetto delle istruzioni impartite

	Errore materiale	Dispersione, perdita e accesso altrui non autorizzato	**M**	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
EVENTI RELATIVI AGLI STRUMENTI	Azione di virus informatici o di codici malefici	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori	**A**	Adozione di idonei dispositivi di protezione
	Spamming o altre tecniche di sabotaggio	Perdita o alterazione di sw o hw con impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**A**	Adozione di idonei dispositivi di protezione
	Malfunzionamento, indisponibilità o degrado degli strumenti	Perdita o alterazione sw o hw; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**A**	Assistenza e manutenzione continua degli elaboratori e dei programmi; ricambio periodico
	Accessi esterni non autorizzati	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**M**	Adozione di idonei dispositivi di protezione
	Intercettazione di informazioni in rete	Dispersione di dati; accesso altrui non autorizzato	**A**	Adozione di idonei dispositivi di protezione
EVENTI RELATIVI AL CONTESTO	Accessi non autorizzati a locali/reparti ad accesso ristretto	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**M**	Protezione dei locali mediante serratura con distribuzione delle chiavi ai soli autorizzati
	Asportazione e furto di strumenti contenenti dati	Dispersione e perdita di dati, di programmi e di elaboratori; accesso altrui non autorizzato	**M**	Protezione dei locali e dei siti di ubicazione degli elaboratori e dei supporti di memorizzazione mediante serratura con distribuzione delle chiavi ai soli autorizzati
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati, dei programmi e degli elaboratori	**M**	Attività di prevenzione, controllo, assistenza e manutenzione periodica,vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it

	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc.)	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**A**	Attività di controllo, assistenza e manutenzione periodica
	Errori umani nella gestione della sicurezza fisica	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	**M**	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione

5 Misure di sicurezza per la protezione dei dati

5.1 Descrizione delle misure di sicurezza fisica

L'edificio dell'Istituto, sito in via Tenente Lusito a Molfetta, è dotato delle seguenti misure:

- Porte antipanico
- Allarme antincendio
- Cancelli a sbarre con apertura a chiave
- Modalità di accesso ai piani tramite ascensore per handicap e scale
- Scale antincendio esterne
- Vigilanza notturna
- Sistema di videosorveglianza

Inoltre sono state poste in essere ulteriori misure:

- Le aree interne, in cui sono conservati i dati (informatici e cartacei), sono protette sia durante l'orario di lavoro che fuori orario in armadi collocati in archivio chiuso a chiave con accesso controllato e comunque consentito solo agli incaricati. Durante l'orario di lavoro il servizio di segreteria assicura l'accoglienza dei terzi che hanno possibilità di accedere alle diverse stanze solo in presenza dell'addetto.
- Negli uffici gli archivi (informatici e cartacei) sono posizionati in armadi chiusi a chiave, ogni ufficio è dotato della propria stampante; tuttavia il sistema di rete, permette l'utilizzo delle stampanti in condivisione. Le stanze in cui sono presenti i fax sono chiuse a chiave in assenza dell'addetto all'ufficio, pertanto non è consentito ad estranei di leggere o asportare, eventualmente, documenti non ancora prelevati dal personale.
- Al di fuori dell'orario di lavoro le aree sono protette mediante chiusura degli spazi. Solo gli incaricati possiedono le chiavi degli archivi contenenti dati sensibili o giudiziari, custodite in luogo sicuro secondo le indicazioni ricevute dal Responsabile del trattamento.

- Le autorizzazioni all'ingresso nei locali vengono concesse sulla base dei compiti assegnati dal piano di lavoro discusso ad inizio d'anno, ogni mutamento o accesso diversificato avviene previa autorizzazione del Dirigente o del DSGA

5.2 Descrizione della rete informatica e delle misure di sicurezza logica

L'Istituto dispone di una propria struttura informatica. Tutte le componenti hardware (dispositivi di connessione, server, client, altri dispositivi) sono stati acquistati in base a caratteristiche di affidabilità e sono periodicamente controllati.
Da tutte le postazioni e da tutti i dispositivi personali (notebook, netbook, tablet, smartphone, smart tv o altro dispositivo provvisto di connessione wi-fi/ethernet) è consentito l'accesso alla rete internet tramite inserimento di credenziali di accesso la cui password è strettamente personale e permette la registrazione, in un file di log, di tutte le attività effettuate in rete che saranno disponibili su richiesta delle autorità competenti. La password di accesso dovrà essere cambiata ogni sei mesi. Si ha, inoltre, accesso alla rete intranet del Ministero, la cui gestione in termini di sicurezza dei dati è del Ministero dell'Istruzione, Università e Ricerca.
L'utilizzo ordinario degli strumenti elettronici è compiuto da personale con privilegi di *"user"*, che non permettono di compiere operazioni che mettano in pericolo il software utilizzato per la gestione dei dati. I privilegi di amministratore sono ad uso esclusivo dell'incaricato al trattamento o di un suo incaricato per il periodo necessario ad effettuare manutenzione hardware e/o software sul sistema.

5.2.1 Protezione virus

Tutti gli elaboratori sono dotati di programma antivirus. Il software antivirus sempre attivo in memoria intercetta tutte le operazioni eseguite dall'utente eseguendo una scansione da virus ogni volta che un file viene aperto; inoltre permette anche controlli a richiesta. Periodicamente o quando necessario vengono eseguite scansioni dai virus conosciuti su tutti i programmi e documenti presenti sul personal computer al fine di permettere la eventuale pulizia dei virus penetrati. Il software copre l'intera struttura informatica della scuola.
Il collegamento di rete è protetto da apposito firewall.

5.2.2 Sistema di autenticazione

Ad ogni incaricato è stata fornita una password di apertura del computer che lo stesso ha provveduto a cambiare con il primo accesso e che ogni sei mesi, se tratta dati comuni, o tre mesi se tratta dati sensibili, provvede autonomamente a cambiare.
L'utilizzo di dette password inibisce ad estranei l'uso dei personal computer, dei programmi e dati in essi contenuti dopo lo spegnimento delle macchine. Durante il tempo in cui esse rimangono accese non è previsto che estranei possano accedervi ed è comunque dotata di password per temporanee assenze del personale. In ogni caso gli incaricati del trattamento sono stati informati e formati sulla gestione della sicurezza dei dati mediante la consegna di precise istruzioni.
Ad ogni incaricato è stato insegnato come cambiare la password del computer ed è stato informato che ogni sei mesi, se tratta dati comuni, o tre mesi se tratta dati sensibili, deve provvedere autonomamente al cambio della stessa. Il gestore delle password avrà quindi il compito di raccogliere (con cadenza semestrale e/o trimestrale) le buste contenenti le nuove password e registrare in apposito modello l'avvenuta modifica della password. In caso di assenza dell'incaricato e di necessità di utilizzare la sua postazione di lavoro, il gestore ha inoltre il compito di chiedere al titolare il permesso di aprire la busta

con la password dell'incaricato ed al ritorno di questo ha l'obbligo di informarlo che la sua password è stata aperta e quindi di invitarlo a fornirne una nuova.
L'utilizzo di dette password inibisce ad estranei l'uso dei personal computer, dei programmi e dati in essi contenuti dopo lo spegnimento delle macchine.
Una volta autenticati, gli utenti hanno accesso solo ai dati e alle applicazioni per le quali sono

incaricati del trattamento. Per l'archiviazione dei documenti generici sul server, ciascun utente dispone di proprie cartelle di destinazione del salvataggio e di cartelle per la condivisione di documenti.
Per rendere le macchine poco vulnerabili sistemi vengono aggiornati periodicamente in modalità automatica.

5.3 Tabella riepilogativa delle misure di sicurezza in essere o da adottare

MISURA	RISCHIO CONTRASTATO	STRUTTURA INTERESSATA	EVENTUALE BANCA DATI INTERESSATA	MISURA GIÀ IN ESSERE	PERIODICITÀ E RESPONSABILITÀ DEI CONTROLLI
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Segreteria Dirigente scolastico	Relativo archivio	Antivirus, credenziali di autenticazione	Bimestrale; responsabile pro tempore del servizio
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Ufficio personale	Relativo archivio	Antivirus, Firewall e credenziali di autenticazione	Bimestrale; responsabile pro tempore del servizio
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Servizi amministrativi	Relativo archivio	Antivirus, Firewall e credenziali di autenticazione	Bimestrale; responsabile pro tempore del servizio

Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Servizi inerenti l'offerta formativa	Relativo archivio	Antivirus, Firewall e credenziali di autenticazione	Bimestrale; responsabile pro tempore del servizio
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Servizi strumentali agli organi collegiali	Relativo archivio	Antivirus, Firewall e credenziali di autenticazione	Bimestrale; responsabile pro tempore del servizio

6 Criteri e modalità per assicurare l'integrità dei dati

In questa sezione sono descritti i criteri e le procedure adottati per il salvataggio dei dati e per il loro ripristino in caso di danneggiamento o di inaffidabilità della base dati.
L'importanza di queste attività deriva direttamente dalla eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che quando sono necessarie le copie dei dati siano disponibili e le procedure efficaci.

6.1 Archivi cartacei

I documenti raccolti su carta sono sempre archiviati all'interno di cartelline non trasparenti. Allo stesso modo vengono conservati i documenti giacenti sulle scrivanie; i quaderni contenenti note od appunti relativi a pratiche in corso sono conservati chiusi e fuori dalla portata di estranei.
Vengono conservati archivi cartacei conservati in armadi chiusi a chiave anche se tutti i dipendenti e collaboratori designati, nel rispetto del segreto professionale, sono autorizzati ad accedere ai dati.
L'accesso ad estranei è sempre controllato grazie alle misure di sicurezza esterne ed alla vigilanza in portineria.
Eventuali copie di documenti, scritti o tabulati di prova sono distrutte manualmente.
La documentazione consegnata a terzi è sempre raccolta in cartelle o buste non trasparenti, previa identificazione del consegnatario e solo in ottemperanza agli obblighi di legge.
I dati sono conservati dalla scuola nei termini di legge.

6.2 Archivi informatici

L'integrità dei dati è garantita, in automatico, utilizzando *"idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni*."
Pertanto le copie di sicurezza vengono aggiornate periodicamente con procedure di salvataggio settimanali.

I supporti di salvataggio delle copie di back-up sono conservate in apposito contenitore conservato in armadio chiuso a chiave. Il back up viene eseguito sotto la responsabilità del responsabile seguendo le istruzioni ripartite. L'amministratore del sistema o persona delegata esegue almeno annualmente un test di verifica dell'efficacia delle prove di sicurezza delle procedure di salvataggio/ripristino dei dati, provando a recuperare files e dati dalle unità di back up.

6.3 Criteri e procedure per la sicurezza della trasmissione dei dati

6.3.1 Dati cartacei

La trasmissione dei fax, tradizionali, qualora non sia possibile inviare elettronicamente la documentazione è effettuata allegando una copertina che individua mittente e destinatario, oggetto e numero di pagine: questo garantisce l'identificazione e rintracciabilità del documento in capo al destinatario.
Sulla medesima copertina inoltre, sono date chiare istruzioni, in caso di errori nella trasmissione, per mezzo della seguente dicitura:
le informazioni, contenute in questo fax, sono da considerarsi solo per uso personale e confidenziale dei destinatari sopra indicati. Questo messaggio può includere dati riservati protetti dal segreto professionale. Se avete ricevuto questa comunicazione per errore datecene notizia immediatamente per telefono e distruggete il documento; ve ne saremo particolarmente grati. Quanto sopra, ai fine del rispetto del D.Lgs 196/03 sulla tutele dai dati personali.
Le copie dei fax inviati mediante apparecchio tradizionale sono riconsegnate a colui che ha eseguito o fatto eseguire la trasmissione, avendo cura di porre, quale primo foglio, il rapporto di trasmissione, formato A4, che viene stampato dal fax, con di seguito i fogli contenente il messaggio; questo garantisce l'identificazione e rintracciabilità del documento in capo al mittente.

6.3.2 Dati elettronici

La trasmissione di documenti tramite posta elettronica avviene attraverso programmi di gestione posta. Per la trasmissione di dati sensibili e/o giudiziari ci si avvarrà dello strumento della posta elettronica certificata.

7 Formazione

Il piano di formazione e sensibilizzazione per informare gli incaricati dei rischi individuati e del trattamento previsto per prevenirne i danni, è attuato in prima istanza tramite apposite riunioni di servizio, mediante le quali vengono illustrate dal Dirigente, dal DSGA e dall'Amministratore di sistema, le problematiche relative alla privacy .
Inoltre sul sito istituzionale nell'Area Docenti è presente un corso di autoformazione rivolto a personale docente e ATA. Sul sito è anche pubblicato il presente documento.
Agli incaricati sono state consegnate le relative istruzioni di trattamento in particolare per le precauzioni da adottare nei trattamenti di dati sensibili e giudiziari.
E' compito del responsabile valutare la necessità dell' aggiornamento del documento e l' organizzare di incontri di formazione e verranno utilizzati i moduli previsti dal sistema qualità.
Compatibilmente con le risorse economiche a disposizione sono previste idonee attività di formazione in

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it

occasione di innovazioni e/o modifiche delle norme e in relazione allo sviluppo scientifico/tecnologico dei mezzi e dei sistemi di protezione.
La formazione è altresì programmata al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

8 Trattamenti affidati all'esterno

Agli enti, agli organismi, alle aziende, alle associazioni, alle strutture accreditate e agli altri soggetti esterni alla Scuola che svolgono parte di trattamenti a seguito di contrattati o convenzioni, viene attribuita la qualità di Responsabile del trattamento ai sensi dell'art. 29 del decreto legislativo 196/2003.
A tali responsabili vengono prescritte le seguenti istruzioni:

- individuare gli incaricati del trattamento e impartire loro istruzioni scritte che garantiscano la liceità, la correttezza e la sicurezza del trattamento in conformità di quanto descritto nelle schede del Regolamento DECRETO N. 305/2006, adottato dal Ministero dell'Istruzione
- attuare, dove necessari, gli obblighi di informazione e acquisizione del consenso nei confronti degli interessati;
- garantire all'interessato l'effettivo esercizio dei diritti previsti dall'art. 7 del decreto legislativo n.196/2003, in ordine all'accesso ai dati e a tutti i diritti di aggiornamento, rettificazione, cancellazione e di opposizione al trattamento;
- adottare tutte le cautele e gli accorgimenti di natura tecnica e organizzativa previsti dal D.Lgs. 196/2003 per assicurare che i trattamenti effettuati avvengano nel pieno rispetto della vigente normativa in materia di privacy e di sicurezza.

Nell'ambito della formalizzazione del contratto di appalto o comunque al momento dell'instaurazione del rapporto di collaborazione, si inseriranno anche i seguenti punti:
1. **Durata del trattamento effettuato dalla Vostra Azienda**. La Vostra Azienda è autorizzata ad effettuare trattamenti di dati per conto di questa scuola, fino al termine di decorrenza del rapporto contrattuale in atto.
2. **Finalità del trattamento effettuato dalla Vostra Azienda**. La Vostra Azienda tratterà i dati esclusivamente per le finalità individuate nel rapporto contrattuale.
3. **Obbligo alla riservatezza**. Con la presente, la Vostra Azienda si impegna a non divulgare, diffondere, trasmettere e comunicare i dati di questa scuola. È titolare del trattamento, se non nelle misura e nelle forme necessarie ad adempiere i termini del rapporto contrattuale in atto.
4. **Titolarità dei dati**. I dati a Voi comunicati sono e rimarranno sempre e comunque di titolarità esclusiva dell'Istituto Tecnico Tecnologico Commerciale "Salvemini" - Molfetta (BA) e pertanto non potranno essere venduti o ceduti, in tutto o in parte, ad altri soggetti, nemmeno alla conclusione del rapporto contrattuale.
5. **Misure minime**. Con la presente la Vostra Azienda si impegna a mettere in atto e a verificare regolarmente l'efficacia di adeguate e preventive misure contro i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità della raccolta, comprese le misure minime di sicurezza fisica, organizzativa e logica prescritte dal D.Lgs. 196/2003.

Conclusione o revoca dell'incarico. All'atto della conclusione o della revoca dell'incarico conferito dall'Istituto Tecnico Tecnologico Commerciale "Salvemini" - Molfetta (BA) alla Vostra Azienda, o in qualsiasi momento Vi venga richiesto per sopravvenute necessità, Vi impegnate a riconsegnare tutti i dati trattati o comunque ricevuti, comprese tutte le copie di backup effettuate e tutta la documentazione cartacea. La Vostra Azienda si impegna altresì a cancellare fisicamente dai propri sistemi e dai propri archivi elettronici e cartacei tutti i dati la cui titolarità è del su citato Istituto.

Via Ten. Lusito, 94 MOLFETTA 70056 (BA) tel./fax 080.334.46.16 - 080.335.43.52 – 080.334.23.28
C.M. BATD04000G - C.F. 80011200724
batd04000g@istruzione.it - batd04000g@pec.istruzione.it - http://www.itetsalvemini.gov.it