DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Indice

4A.1. OGGETTO E FINALITÀ

In questo allegato vengono definiti i criteri e le modalità operative adottate dall'Istituto Scolastico per l'adozione del documento programmatico sulla sicurezza. In particolare vengono descritti i modi per individuare e valutare i rischi e quindi adottare le misure adeguate alla protezione della sicurezza delle aree, dei dati e delle trasmissioni, al fine di ridurre al minimo i rischi stessi.

4A.2. APPLICABILITÀ

Le indicazioni contenute nel presente documento devono essere utilizzate per gestire i rischi connessi alle attività di trattamento dei dati personali, in seno all'Istituto Scolastico, ma anche da parte dei responsabili esterni.
Le attività di trattamento prevedono, oltre le tipologie ricorrenti (raccolta, registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione), particolari forme nel caso di dati sensibili e giudiziari, secondo quando indicato nelle schede allegate al Regolamento (D.M. 305/2006).

4A.3. RIFERIMENTI NORMATIVI

Articolo	Norma
Art. 31	D.Lgs. n. 196/2003
Art. 33- 34-35-36	D.Lgs. n. 196/2003
Allegato B Punti da 19.1. a 19.8	disciplinare tecnico D.Lgs. n. 196/2003
Allegato B Punto 25	D.Lgs. n. 196/2003
Art. 180 (disposizioni transitorie)	D.Lgs. n. 196/2003
Regolamento sul trattamento dei dati sensibili e giudiziari e schede allegate (D.M. 305/2006)	

4A.4. RESPONSABILITÀ

Il titolare è responsabile dell'analisi e della valutazione dei rischi ai fini dell'adozione delle misure di sicurezza, sia idonee, sia minime. Il titolare si avvale del Gruppo Privacy per la predisposizione della presente modulistica qualora venga nominato tale organo che, seppur non previsto dalla legge, è ritenuto importante per l'applicazione effettiva degli adempimenti previsti dalla legge. In particolare il Dirigente scolastico, Titolare del trattamento, deve adottare le misure minime, ai sensi del disciplinare tecnico del D.Lgs. 196/2003, e procedere alla predisposizione delle misure idonee ritenute indispensabili nella struttura di afferenza. Spetta al titolare del trattamento, coadiuvato dall'eventuale Gruppo Privacy, valutare la congruità tecnico-economica delle misure proposte e quindi disporre l'adozione delle stesse.

4A.5. CRITERI PER L'INDIVIDUAZIONE DEI RISCHI

Occorre innanzitutto premettere che gli articoli da 33 a 36 del Testo Unico in materia di Trattamento dei dati personali di cui al D.Lgs. 30 giugno 2003 n. 196 prevedono l'obbligo di adottare le misure minime di sicurezza.
Tali misure debbono essere obbligatoriamente adottate ai sensi dell'allegato B del disciplinare tecnico del Testo Unico e ciò in base all'individuazione di due grandi categorie di rischi:

A. Rischi connessi al mancato rispetto degli adempimenti e delle prescrizioni statuite dal Nuovo Testo Unico in materia di trattamento di dati personali;
B. Rischi propri del sistema informatico utilizzato dall'Istituto Scolastico.

Tale distinzione si chiarisce se si considera che i rischi del trattamento della prima categoria si riferiscono direttamente ed unicamente all'intera materia inerente la tutela dei dati personali mentre i rischi sottesi alla seconda si riferiscono all'applicazione pratica, effettiva e funzionale delle misure di sicurezza adottate, tra queste comprese quelle relative alla sicurezza informatica.
L'analisi del rischio è stata, pertanto, affrontata secondo quanto sopra riportato e consequenzialmente suddivisa in due settori di rischi propri nettamente differenti e separati per tipologia e materia.

PRIMO SETTORE DI RISCHIO:
In questa fase dell'analisi sono stati individuati e valutati tutti i rischi previsti dalla legge, quali, ad es. il rischio di distruzione accidentale dei dati, il rischio di perdita dei dati, il rischio di accesso non autorizzato, il rischio di trattamento di dati non conforme alla finalità della raccolta, il rischio di trattamento illegittimo e di trattamento non consentito, ecc. che sono potenzialmente insiti in ogni istituto scolastico. Si pensi ad esempio alla comunicazione a terzi ed in particolare a privati di dati personali degli alunni al fine di agevolarne l'orientamento, la formazione e l'inserimento professionale e ciò nonostante i dati personali siano stati raccolti per il soddisfacimento delle esclusive finalità afferenti l'istruzione.
Ebbene, si è potuto constatare anche che quanto sopra riportato integra una forma di trattamento illegittimo di dati alla stessa stregua di prassi di comunicazione di dati relativi agli esiti scolastici di studenti, siano essi intermedi che finali. A tal proposito è stato constatato che tali prassi, pur se oramai consolidate, al fine della loro legittimità necessitano di ulteriori prescrizioni e di specifiche richieste degli alunni ai sensi ed agli effetti dell'art. 96 del D.Lgs n.196/2003 al fine di evitare trattamenti non autorizzati di dati, non conformi alle finalità della raccolta nonché comunicazioni di dati personali non previste preventivamente dalla legge.
A tal proposito si è ritenuto fondamentale arginare il menzionato problema innanzitutto con una specifica analisi del flusso dei dati e dei soggetti ai quali sono comunicati nonché con un adeguato ed efficiente piano di formazione degli incaricati del trattamento e ciò in quanto è dato riscontrare anche dalle informazioni e dalle notizie di cronaca che la maggior parte delle violazioni della privacy vengono perpetrate direttamente e quasi unicamente dagli incaricati del trattamento i quali, viceversa, al fine di applicare correttamente i principi sottesi dalla legge e le procedure adottate dall'Istituto scolastico, debbono conoscere a quali soggetti e con quali modalità i dati possono essere comunicati dalla segreteria scolastica verso l'esterno.
Dall'analisi del novero dei trattamenti effettuati nella segreteria dell'Istituto scolastico è emersa anche la necessità di porre particolare cautela ad azioni potenzialmente diffusive di dati personali nonostante le stesse non siano preordinate a rendere informazioni come ad esempio quelle di lasciare, sia pur provvisoriamente, documenti contenenti dati personali su un bancone della segreteria posto a diretto contatto con il pubblico. Ulteriore azione potenzialmente diffusiva è quella di cestinare un semplice documento cartaceo senza provvedere alla sua distruzione e ciò in quanto fuoriuscendo tale documento dal controllo dell'Istituto scolastico potrebbe essere conosciuto da un numero indeterminato di soggetti che, utilizzandolo per scopi personali, potrebbero, a ben vedere, causare danni a volte difficilmente immaginabili e con conseguenze anche estremamente dannose nel caso in cui il documento contenesse dati personali sensibili e/o giudiziari.
E' stato ritenuto necessario corredare la segreteria di appositi distruggidocumenti cartacei nonché di formare adeguatamente il relativo personale ATA poiché a diretto e continuo contatto con il pubblico al quale potrebbero, sia pur inconsapevolmente, essere comunicati o diffusi

illegittimamente dati personali in assenza di specifica conoscenza della legge sul trattamento dei dati personali.
Di tale settore di rischio è necessario occuparsi, quindi, mediante l'approfondita conoscenza della legge sulla Privacy e del Regolamento sul trattamento dei dati sensibili e giudiziari (D.M. 305/2006).
Si è ritenuto, infatti, che solo un'adeguata conoscenza del disposto normativo possa realmente e proficuamente garantirne l'osservanza del medesimo ed in definitiva possa abbattere effettivamente i rischi connessi a tale primo settore che, anche in base all'analisi della mancata registrazione di violazioni del trattamento informatico e cd. cartaceo, è stato concordemente ritenuto il più rilevante ed in definitiva quello avverso il quale dedicare le maggiori attenzioni per garantire trattamenti dei dati degli alunni e del personale docente in conformità alle prescrizioni legislative.
L'analisi del rischio è stata, pertanto, affrontata secondo quanto sopra riportato e consequenzialmente suddivisa in due settori di rischi propri nettamente differenti e separati per tipologia e materia.

SECONDO SETTORE DI RISCHIO:
In questa fase, invece, sono stati identificati e valutati i rischi del sistema informatico e tutti quelli che sono propri della sua normale attività.

Da ciò consegue che proprio nella fase di valutazione dei rischi si devono verificare:
a) l'efficacia degli strumenti impiegati al fine di assegnare al rischio un indice di gravità (quali danni sono stati riscontrati o quali ancora possibili) e di frequenza (intesa a verificare, nonostante la misura adottata) e quindi di individuare le circostanze di manifestazione di attacchi informatici al fine di individuarne anche le consequenziali azioni correttive;
b) le misure che sono risultate non adeguate.

Il processo di individuazione ed ulteriore valutazione dei rischi eventualmente manifestatisi deve essere ripetuto con cadenza almeno annuale e, comunque, immediatamente al verificarsi di rischi gravi connessi al trattamento o segnalati dall'installatore esterno delle misure minime di sicurezza.

Le misure minime di sicurezza devono tendere a ridurre al minimo 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. L'adeguatezza delle misure deve essere valutata, secondo le linee guida indicate in questo documento, tenendo conto delle conoscenze acquisite in base al progresso tecnico, alla natura dei dati trattati e alle specifiche caratteristiche del trattamento. A tal proposito si è proceduto all'individuazione dei rischi utilizzando le apposite matrici (MAS XX), in cui sono riportati i singoli fattori di rischio: questi sono divisi rispettivamente tenendo conto dei rischi relativi alle aree e locali, all'integrità dei dati e alle trasmissioni. Le matrici sono utilizzate come uno strumento elastico: i singoli responsabili possono adattarle in base all'esperienza maturata, all'anamnesi e alle caratteristiche specifiche dei trattamenti. Si potrà procedere all'analisi dei rischi settore per settore. Si è proceduto all'analisi facendo attenzione a non considerare le misure già adottate: l'analisi è stata fatta con un sistema cd. a protezione zero, valutando astrattamente quali possono essere i rischi, a prescindere dalle misure che sono state già adottate. Ciò serve a verificare se quanto fatto è da considerarsi idoneo, oppure necessiti di interventi adeguativi.

4A.6. CRITERI PER LA VALUTAZIONE DEI RISCHI

Una volta individuati i rischi si è proceduto alla valutazione degli stessi, attraverso una indicizzazione delle possibili perdite. In particolare si è tenuto conto di due indici:

- **probabilità (P) di accadimento**, che riguarda la frequenza riscontrata o riscontrabile;
- **magnitudo (M) delle conseguenze**, nel caso lo stesso evento si verifichi.

Il Rischio altro non è che la risultante della probabilità e della gravità di un evento: **l'indice R è quindi dato dal prodotto P X M.**
Secondo i criteri adottati dando a **P** un valore fra 1 e 4 e a **M** ugualmente fra 1 e 4, si è ottenuto il valore **R** compreso fra 1 e 16.

Probabilità (P)

1: Improbabile	Non sono noti episodi.
2: Poco probabile	Sono noti rarissimi episodi.
3: Probabile	Noto qualche episodio in cui la mancanza rilevata ha fatto seguito a un danno.
4: Altamente probabile	Si sono verificati danni per la stessa mancanza rilevata in situazioni simili.

Magnitudo (M)

1: Lieve	Furto o distruzione dei dati
2: Medio	Utilizzo illegale o alterazione dei dati
3: Grave	Perdita di dati causata da un uso non autorizzato da parte di un dipendente.
4: Gravissimo	Perdita dei dati a seguito di diffusione illegale.

L'avere fatto l'analisi a cd. protezione zero consente di verificare il grado di efficacia delle misure già adottate. Un esempio può essere utile a chiarire: essere dotati di un **firewall** comporta che non si possa eludere il rischio di attacchi esterni da parte di hacker (circostanza per la quale non può dirsi di essere al sicuro in assoluto). Il sistema di analisi a cd. protezione zero comporterà che il rischio di attacchi è comunque preso in considerazione, a prescindere dalle misure adottate. Sarà invece in sede di valutazione che si dovranno verificare:

a) l'efficacia degli strumenti adottati, attraverso l'analisi dei cd. file di log, al fine di assegnare al rischio un indice di gravità (quali danni si sono avuti o quali possano essere possibili) e di frequenza (intesa a verificare, nonostante la misura adottata); quali siano state le circostanze in cui si sono subiti attacchi;
b) le misure che sono risultate non adeguate.

Il processo di individuazione e valutazione dei rischi deve avvenire con cadenza al massimo annuale, ma può essere ripetuto anche nel corso dell'anno.

4A.7. MISURE DI PREVENZIONE E PROTEZIONE

Le azioni necessarie per l'adozione di idonee misure di sicurezza riguardano:

a) **la prevenzione:** attività che permette di impedire gli accadimenti negativi, agendo direttamente sulla diminuzione delle probabilità di manifestazione dei pericoli;
b) **la protezione:** attività che permette di diminuire la gravità degli effetti causati eventualmente dall'accadimento dell'evento di pericolo.

Dopo aver analizzato e valutato i fattori di rischio, relativi alle aree e locali, all'integrità dei dati e alle trasmissioni, sono state individuate le misure di prevenzione e protezione più idonee a ridurre o eliminare il rischio stesso.
L'insieme delle misure preventive e protettive costituisce un programma di fondamentale importanza nell'ambito della politica per la Sicurezza, poiché fornisce una guida operativa, che permette di gestire la Sicurezza con organicità e sistematicità e in modo dinamico. Per definire uno scadenzario degli interventi l'Istituto Scolastico ha adottato un criterio di "n" mesi crescenti in funzione inversa all'indice di gravità (e quindi al valore del numero "R").
Vedere esempio seguente:

- **R = 16** intervento entro 01 mesi e verifica entro 10 giorni
- **R = 12** intervento entro 04 mesi e verifica entro 20 giorni
- **R = 08** intervento entro 08 mesi e verifica entro 30 giorni
- **R = 04** intervento entro 12 mesi e verifica entro 40 giorni
- **R = 01** intervento entro 16 mesi e verifica entro 60 giorni.

Il programma delle misure di sicurezza adottate o da adottare (riportato in MAS 04.03 – MAS 04.04 – MAS 04.05) per ogni categoria di rischi (aree e locali, integrità dei dati e trasmissioni) è sistematicamente aggiornato nell'ottica di un miglioramento continuo del Sistema Sicurezza dell'Istituto Scolastico: esso è sottoposto a riesame ogni anno, salvo diversa indicazione del titolare del trattamento o per iniziativa dei responsabili, che riscontrino necessità di intervento o non conformità (tecniche o normative). Obiettivo delle misure programmate è comunque ridurre al minimo valore possibile l'indice di rischio relativo "R" a seguito dell'adozione, da parte dei singoli responsabili, delle misure idonee di protezione proposte al Titolare del Trattamento.

Misure Organizzative			
01	Analisi dei rischi	07	Misure graduate per classi dati
02	Redazione linee-guida sicurezza	08	Consultazioni registrate
03	Istruzioni interne	09	Controlli periodici
04	Assegnazione incarichi	10	Verifiche periodiche per finalità
05	Formazione professionale	11	Sorveglianza sulla distruzione sup.
06	Classificazione dei dati	12	Altro

Misure Fisiche			
01	Vigilanza della sede	07	Deposito in cassaforte
02	Ingresso controllato	08	Custodia in armadi blindati
03	Sistemi di allarme	09	Dispositivi antincendio
04	Registrazione accessi	10	Continuità elettrica
05	Autenticazione accessi	11	Verifica leggibilità supporti
06	Custodia in classificatori o armadi	12	Altro

Misure Logiche			
01	Identificazione utente	09	Annotazione fonti dei dati
02	Autenticazione utente	10	Annotazione responsabile operaz.
03	Controllo accessi	11	Rilevazione intercettazioni
04	Registrazione accessi	12	Monitoraggio continuo sessioni
05	Controlli antivirus	13	Sospensione automatica sessioni
06	Sottoscrizione elettronica	14	Verifiche automatizzate dati
07	Cifratura dati trasmessi	15	Controllo supporto dati manutenz.
08	Cifratura dati memorizzati	16	Altro

4A.8. PROGRAMMA DELLE MISURE DI PREVENZIONE E PROTEZIONE

Il programma delle misure di protezione necessarie per il trattamento dei rischi analizzati e valutati, in base ad un criterio quantitativo, sono riportate nelle ceck-list utilizzate per la gestione dei rischi, con la definizione dei tempi previsti per l'adozione. Sono state previste anche le modalità per la verifica dell'adozione delle misure programmate e per il monitoraggio della idoneità delle stesse. Qualora sia stato nominato il Gruppo Privacy, i suoi componenti o, personale esterno ed indipendente, possono essere incaricati, da parte del Titolare del Trattamento, di svolgere verifiche periodiche, anche mediante visite ispettive, finalizzate a controllare il rispetto degli standard di sicurezza dell'Istituto Scolastico.

4A.8.1 Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati personali.

Il presente paragrafo è stato elaborato in riferimento al punto 19.5 del disciplinare tecnico del D.Lgs. 196/2003 che impone la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23.
Il successivo punto 23 richiamato stabilisce inoltre che "sono adottate 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".
Considerato che ogni sistema informatico deve prevedere un piano di emergenza per soddisfare le specifiche del disciplinare tecnico è necessario, pertanto, riferirsi alle procedure già applicate ed in particolare alla dichiarazione di responsabilità dell'installatore/i esterno dell'Istituto scolastico per quel che riguarda le misure minime di sicurezza del trattamento dei dati personali e tra queste quelle previste per le copie di back-up.
Quanto affermato muove dalla considerazione che ogni giorno leggiamo di nuovi virus che si propagano rapidamente e che gli stessi sono causa di notevoli danni che a volte raggiungono proporzioni gigantesche.

Il Dirigente scolastico ed il Responsabile del trattamento dei dati personali dell'Istituto Scolastico hanno prestato molta attenzione a questo delicato problema ed hanno ben ritenuto di prevedere una serie di procedure di recupero immediato dei dati in caso di attacchi e, comunque, delle copie di salvataggio periodiche dei dati personali trattati.
Per il raggiungimento di tale obiettivo sono state correttamente analizzati e testati tutti i software in possesso dell'Istituto scolastico, tutti gli hardware nonché tutti gli altri strumenti informatici tecnico-operativi dell'intero sistema informatico scolastico.
Devesi comunque rilevare che nel campo dell'insegnamento non sono state mai registrate problematiche in ordine al trattamento dei dati personali e ciò nonostante, il Dirigente Scolastico non ha mai tralasciato, comunque, l'aspetto della sicurezza e della protezione dei dati personali per la quale si precisa, pertanto, che già da parecchi anni sono state applicate e predisposte tutta una serie di contromisure e tra queste quelle delle copie di back-up periodiche evidenziate nella dichiarazione ai sensi dell'art. 180 del D.Lgs. n. 196/2003 e che le medesime vengono costantemente aggiornate.

4A.9. interventi formativi degli incaricati del trattamento.
4A.9.1 Scopo della formazione.

Il dirigente scolastico ha ritenuto che la previsione degli interventi formativi degli incaricati del trattamento rientra tra gli aspetti più importanti del presente documento programmatico sulla sicurezza e ciò in quanto può realmente parlarsi di effettiva sicurezza del trattamento solo in costanza di un dettagliato piano di formazione degli incaricati.
Alla stregua delle altre materie e degli adempimenti previsti a carico del personale insegnante e non, la formazione è stata ritenuta alla stessa stregua di un elemento fondamentale per il raggiungimento degli obiettivi prefissati ed in particolare per quello della sicurezza del trattamento dei dati personali.
Da quanto evidenziato ne consegue che la predisposizione e l'applicazione di sofisticati strumenti di sicurezza, informatica e non, non garantiscano la stessa in
modo assoluto senza le capacità e/o le adeguate conoscenze del personale ATA chiamato alla loro gestione nonché anche del corpo insegnante per quel che attiene il trattamento dei dati degli alunni effettuato con i registri di classe. Difatti, una gestione impropria da parte di tali soggetti, la mancanza di chiare direttive esplicative e l'assenza di strumenti di controllo di facile e rapida applicazione costituiscono le cause principali per la verificazione anche inconsapevole di danni agli interessati ed in definitiva la causa prioritaria di trattamenti illegittimi e non conformi alle specifiche finalità dell'istruzione scolastica.
Quanto premesso trova effettivo riscontro nel comma 19.6. del D.Lgs. 196/2003 che impone, infatti, "la previsione di 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 formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali."

4A.9.2 Tecniche di formazione degli incaricati del trattamento dei dati personali.
Tra gli aspetti salienti della disamina degli interventi formativi degli incaricati del trattamento il Dirigente scolastico ha ritenuto necessario ed indispensabile prevedere un adeguato e dettagliato piano di formazione del personale ATA quale incaricato del trattamento dei dati personali e del corpo docente.
Tale intervento formativo è stato predisposto ed applicato sotto la diretta vigilanza e la coordinazione del Responsabile del Trattamento.
Tale indispensabile strumento del Documento Programmatico sulla sicurezza è articolato in più lezioni in ognuna delle quali devono essere affrontati specificamente e dettagliatamente gli aspetti più delicati della legge sulla Privacy e sulle misure di sicurezza e ciò al fine di permetterne vari approfondimenti nonché riflessioni e dibattiti.
Per quel che concerne gli insegnanti devesi rilevare come gli stessi debbano prestare la massima attenzione a custodire il registro di classe durante le ore di lezione, a non permetterne la sua

consultazione a soggetti non autorizzati nonché a conservare tale registro al termine delle lezioni negli appositi siti predisposti nella sala insegnanti.
Tra le varie tecniche didattiche il Titolare ed il Responsabile del Trattamento dei dati personali dell'Istituto scolastico hanno ritenuto più proficua quella della lezione tenuta direttamente dal Responsabile del trattamento medesimo in base alla sua specifica conoscenza della materia della Privacy e ciò con il supporto di materiale cartaceo esplicativo della Legge sul trattamento dei dati personali e del Regolamento sul trattamento dei dati sensibili e giudiziari. Copia del materiale esplicativo deve essere consegnato agli incaricati presenti alle lezioni di formazione al fine della migliore e più completa comprensione della materia e degli adempimenti richiesti dalla medesima nonché delle misure minime di sicurezza applicate dall'Istituto scolastico.

4A.9.3 Valutazione dell'efficienza del piano di formazione

Il Dirigente scolastico ed il Responsabile del Trattamento dei dati personali dopo avere dettagliatamente individuato il contenuto del piano di formazione del personale ATA e degli insegnanti hanno ritenuto ulteriormente importante approntare una serie di strumenti di verifica dell'efficienza della formazione per essere certi che la formazione impartita sia stata realmente recepita dagli incaricati del trattamento e che sia stata determinante ad un appropriato e sicuro trattamento dei dati personali.
Si è ritenuto che la formazione possa affermarsi e dirsi veramente tale solo se in grado di soddisfare le esigenze dell'Istituto scolastico per la salvaguardia delle quali è stata prevista l'utilizzazione di un questionario da sottoporre ai partecipanti a fine corso per effettuare una dettagliata valutazione dell'efficacia del loro apprendimento.

4A.9.4 Aggiornamento e programmi individuali di formazione.

Dopo avere affrontato nel dettaglio l'importanza di tale adempimento deve, comunque, ricordarsi che la formazione deve essere sempre aggiornata in base al disposto del D.Lgs n. 196/2003 in coincidenza con l'obbligo di aggiornamento del Documento Programmatico sulla Sicurezza. Deve tenersi ben presente una chiara distinzione tra:

A) AGGIORNAMENTO PERIODICO
B) AGGIORNAMENTO SPECIFICO

Per il quale l'aggiornamento periodico deve essere adempiuto sotto la diretta vigilanza del Responsabile del Trattamento con cadenza almeno annuale e quello specifico, viceversa, tempestivamente effettuato ogni qualvolta l'incaricato sia deputato a trattare nuove banche dati oppure utilizzi nuovi strumenti informatici e/o nuove e diverse procedure.
Muovendo da questa considerazione ne discende che se l'incaricato viene assegnato a nuove mansioni o se viene trasferito da un settore ad un altro deve essere effettuato un nuovo e specifico aggiornamento mediante un programma individuale che deve essere impartito dal Responsabile in relazione alla nuova e specifica attività di trattamento svolta.

4A.10 Misure di sicurezza suppletive relative al trattamento di particolari dati sensibili.

Il presente paragrafo evidenzia le ulteriori misure in caso di trattamento di dati sensibili o giudiziari richieste dal disciplinare tecnico del D.Lgs. n. 196/2003 ed in particolare dal punto 19.8. per i dati personali idonei a rivelare lo stato di salute. Vengono, pertanto, individuati dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.
Una breve parentesi è necessaria per comprendere nel dettaglio gli adempimenti da effettuarsi ed in particolare un riferimento al punto 20 del disciplinare tecnico secondo quale" I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici" ed il successivo punto 21 che stabilisce, inoltre, che "sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti", oltre ancora il punto 22 secondo il quale "i supporti
rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati

al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili".
Per quanto riportato nel detto disciplinare il punto 23 prescrive che "sono adottate 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.
Per quanto sopra riportato non v'è dubbio che la protezione crittografica dei dati cui si riferisce lo stesso Testo Unico in materia di trattamento di dati personali rappresenti un prezioso strumento di tutela e di sicurezza contro i rischi di accesso ai dati personali.
Deve porsi particolare attenzione al trattamento dei dati sensibili poiché debbono essere archiviati nel sistema informatico centrale con estrema sicurezza perché l'accesso alla consultazione e/o alla modificazione dei dati sensibili sarà sempre condizionato dal rispetto della procedura di identificazione degli incaricati ed in definitiva dei seguenti criteri in base ai quali:
a. L'incaricato deve essere precisamente individuato ed autenticato;
b. L'incaricato può trattare i dati sensibili solo con un appropriato profilo di autorizzazione;
c. L'incaricato deve essere in possesso della chiave di lettura o cifratura.
Per quanto detto e per le menzionate procedure gestionali dei dati sensibili deve evidenziarsi in definitiva che i dati sensibili debbono essere nettamente separati e gestiti autonomamente ed indipendentemente da ogni incaricato unicamente in base al proprio profilo di autorizzazione e per quel che attiene i dati personali degli alunni riportati sul registri didattici prevedere che, al termine dell'ultima lezione del giorno, l'insegnante abbia cura di riporre i relativi registri nello specifico sito presente nella sala insegnanti.

4A.11. ALLEGATI

MAS 04.02	DPSS protezione trasmissione dati
MAS 04.03	DPSS protezione trasmissione dati automatizzati
MAS 04.04	DPSS protezione integrità dati automatizzati
MAS 04.05	DPSS protezione aree e locali
MAS 04.12	Report virus
MAS 04.13	Report annuale rischi hardware
MAS 04.14	Report annuale rischi nelle applicazioni
MAS 04.15	Report annuale rischi sistemi operativi
MAS 04.16	Report annuale rischio luoghi ove vengono trattati i dati