Distretto Scolastico 11°
IX CIRCOLO DIDATTICO STATALE
JAPIGIA I
Plesso San Francesco Via Peucetia n. 50 BARI – Tel. 0805530943/5541991 fax 080 5524042
Plesso Don Orione Viale Japigia n.140 BARI – Tel./Fax 0805537467
E mail: BAEE009008@istruzione.it Web: www.circolojapigia1bari.it
C.M.BAEE009008 ***C.F. 80023130729***

D.P.S.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

A.S.2008/2009

SEZIONE I

Note generali

Art.1

Documento programmatico sulla sicurezza

Il presente Documento è Predisposto ai sensi dell'art. 34, comma 1, punto g, del Decreto legislativo 30 giugno 2003, n.196, e dell'allegato B, Disciplinare Tecnico in materia di misure minime di sicurezza, regola 19.

Art.2

Finalità del documento

Con il presente documento si definiscono le politiche e gli standard di sicurezza in merito al trattamento dei dati personali effettuato da questa Istituzione scolastica, Titolare del trattamento, individuando le misure di sicurezza minime adottate nonché quelle da adottare per garantire il rispetto della normativa e, conseguentemente, il rispetto dei diritti individuali dei soggetti interessati dal trattamento.

Art.3

Oggetto del documento

Il D.P.S. trova attuazione nei confronti di qualsiasi trattamento di dati personali effettuato con l'ausilio di computer o di altri strumenti elettronici di elaborazione nonché mediante supporti cartacei ed audiovisivi.

I dati personali sono distinti in: **dati comuni**; **dati sensibili**; **dati giudiziari.**

Al fine di predisporre un corretto sistema di tutela dei dati personali, nel presente documento vengono evidenziati:

a) La struttura scolastica;

b) i trattamenti effettuati dalla scuola;

c) l’organizzazione interna con l’individuazione e la suddivisione dei compiti e delle responsabilità tra il personale dell’Istituto;
d) i rischi che incombono sui dati e le misure, adottate o da adottare, per prevenire la realizzazione degli stessi;
e) i criteri e le modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
f) il piano degli interventi formativi;

Art.4
Campo di applicazione

Tutti i settori della scuola (didattico, organizzativo, amministrativo) devono avere conoscenza del presente Documento al fine di una corretta applicazione dello stesso.

Art.5
Responsabile del procedimento

Il Dirigente scolastico ROSSINI Patrizia, rappresentante legale pro-tempore dell’Istituto, ha seguito di un’attenta valutazione dei trattamenti effettuati dall’Istituto nonché della struttura organizzativa, ha ritenuto opportuno individuare quale Responsabile per il trattamento dei dati personali il sig. LAVOPA Lorenzo, Direttore dei Serv. Gen. ed Amm.vi, codice fiscale LVPLNZ65A07A662S, nominato con nota 2956/B32 del 31/03/2009;

La nomina è a tempo indeterminato e il responsabile può decadere per revoca, dimissioni o trasferimento. Resta salva la possibilità per il Dirigente scolastico di revocare la nomina senza preavviso e di procedere all’individuazione di un nuovo responsabile.

Il responsabile sopra indicato ha collaborato alla redazione del presente documento e lo firma in calce allo stesso.

Art.6

La struttura scolastica

Il IX° CIRCOLO DIDATTICO JAPIGIA I si compone di due (2) plessi di seguito elencati, per ciascuno dei quali si evidenziano i dati relativi alla sede, al personale e d agli alunni.

1) **Sede Centrale: Plesso di Scuola Primaria e dell'Infanzia San Francesco**

   L'edificio è ubicato nel comune di Bari in Via Peucetia n.50, ed è la sede del Dirigente scolastico e del D.S.G.A. Nel plesso frequentano 366 alunni e lavorano 36 docenti, 4 assistenti amministrativi e 8 collaboratori scolastici.

2) **Sede distaccata: Plesso Scuola Primaria e dell'Infanzia DON ORIONE**

   L'edificio è ubicato nel comune di Bari in Viale Japigia n.140. Nel plesso frequentano 396 alunni e lavorano 41 docenti e 9 collaboratori scolastici.

SEZIONE II

Trattamento dei dati personali

Titolo I

Soggetti interessati al trattamento

Art.7

Elenco dei dati personali trattati

In questo Istituto scolastico vengono trattati i dati:

a) degli alunni ed delle loro famiglie;
b) del personale dipendente della scuola;
c) del personale esterno utilizzato per collaborazioni professionali;
d) dei fornitori di beni e servizi.

Inoltre, occorre evidenziare il trattamento dei dati relativi alla gestione finanziaria, alla gestione del programma annuale, alla gestione istituzionale, al protocollo informatico nonché il trattamento dei dati effettuato con il marcatempo elettronico.

Infine rileva anche il trattamento dati relativo alla gestione del sito Web della scuola, con l'utilizzo dei dati degli alunni.

Per tutti i dati appena elencati, negli articoli che seguono saranno evidenziati:

a) il tipo di trattamento e la relativa finalità;
b) la natura dei dati trattati;
c) la struttura o le strutture di riferimento (ossia preposte al trattamento);
d) l'utilizzo degli strumenti elettronici.

Art.8
Dati degli alunni

Relativamente ai dati degli alunni occorre distinguere tra due diverse tipologie di trattamento.

a) Trattamento dati la cui finalità concerne la didattica e altre attività correlate, integrative e complementari.

   I dati trattati in questo ambito hanno natura comune. Non è da escludere la possibilità di trattare dati sensibili (gestione dell'ora di religione) con particolare riferimento allo stato di salute (problematiche attinenti gli alunni diversamente abili, diagnosi funzionali). Particolari situazioni concernenti gli alunni possono determinare la necessità di trattare dati giudiziari (provvedimenti di affido, di allontanamento del minore, ecc.).

   La struttura di riferimento è individuata nel corpo docente. Questo è coadiuvato dal Dirigente scolastico, dal D.S.G.A. e dalla Segreteria.

   A livello informatico vengono utilizzati computer con software gestionale e con programmi di elaborazione testi. Non è prevista alcuna comunicazione telematica.

b) Trattamento dati finalizzato alla gestione dell'attività amministrativa e delle altre attività correlate, integrative e complementari. Tale trattamento concerne, in particolare, la gestione dei dati per le attività di supporto alla didattica, per l'organizzazione ed il funzionamento della scuola. In questo ambito è da comprendere il trattamento dei dati degli alunni per la stipula di assicurazioni al fine di una corretta gestione degli infortuni nonché il trattamento finalizzato ad una corretta attuazione del D.Lgs. 81/08.

   I dati trattatati hanno natura comune. Non è da escludere, come visto alla lett. a), la possibilità di trattare dati sensibili, con particolare riferimento allo stato di salute. Nonché dati giudiziari (v.lett. a).

   La struttura di riferimento è individuata nella Segreteria e nel D.S.G.A. Questi sono coadiuvati dal Dirigente scolastico e dai suoi collaboratori, dai collaboratori scolastici.

   A livello informatico vengono utilizzati computer con software gestionale e con programmi di elaborazione testi. Attualmente la comunicazione telematica

concerne dati statistici anonimi (numero delle classi, degli organici, degli alunni iscritti). Potrebbe riguardare dati personali anche di natura sensibile: si pensi alle comunicazioni tra scuola e comune (fruizione della mensa gratuita per gli alunni appartenenti a famiglie in condizioni economiche sfavorevoli) o alle comunicazioni tra scuola e A.s.l. (in materia di diagnosi funzionali).

Il trattamento di cui alla lett. a) e b) è esteso ai dati concernenti le famiglie degli alunni.

Art.9
Dati del personale dipendente della scuola

Il trattamento dei dati concernenti il personale dipendente viene effettuato per le seguenti finalità:

a) attività amministrativa e attività correlate (con riferimento anche ai dati delle loro famiglie);
b) motivi disciplinari;
c) attività retributiva e previdenziale (con riferimento anche ai dati delle loro famiglie);
d) organizzazione e funzionamento della scuola;
e) gestione infortuni e malattie professionali, assicurazione, corretta attuazione del D.Lgs. 81/08.

I dati trattati hanno natura comune. Non è da escludere la possibilità di trattare dati sensibili, con particolare riferimento allo stato di salute. Possibilità di trattare in ipotesi specifiche anche dati giudiziari.

La struttura di riferimento è individuata nella Segreteria e nel D.S.G.A. Questi sono coadiuvati dal Dirigente scolastico e dai suoi collaboratori, dai collaboratori scolastici.

A livello informatico vengono utilizzati computer con software gestionale e con programmi di elaborazione testi. La trasmissione telematica concerne: comunicazioni scioperi personale, contratti individuali di lavoro del personale, inserimento dati costituzione graduatorie interne di circolo, dati organico personale docente e non docente, comunicazioni relative agli stipendi e compensi accessori del personale (INPS-INPDAP-DPT- MINISTERO ECONOMIE E FINANZA). Comunque dati non sensibili e non giudiziari.

Art.10
Dati del personale esterno utilizzato per collaborazioni professionali

I trattamento evidenziato nel presente articolo concerne i dati del personale esterno utilizzato in collaborazioni professionali: si pensi ad educatori, formatori, consulenti. Il trattamento è necessario per le seguenti finalità: amministrativa, retributiva, previdenziale, fiscale e per tutti gli argomenti connessi con le stesse finalità.

I dati trattati hanno natura comune ma non è da escludere la possibilità di trattare dati giudiziari.

La struttura di riferimento è rappresentata dal D.S.G.A. e dagli assistenti amministrativi. Sono coadiuvati dal Dirigente scolastico ed, eventualmente, dal collaboratore del Dirigente.

A livello informatico vengono utilizzati computer con software gestionale e con programmi di elaborazione testi. La comunicazione telematica avviene nei confronti del Ministero dell'Economia e delle Finanze (per ciò che concerne l'anagrafe delle prestazioni) e del MIUR (per ciò che concerne i flussi finanziari). Solo dati comuni

Art.11
Dati dei fornitori di beni e servizi

I trattamento qui evidenziato concerne i dati dei fornitori di beni e servizi della scuola (manutenzione computer, servizio mensa, servizio trasporto, ecc.). Il trattamento è necessario per finalità di natura amministrativa e fiscale e per tutti gli argomenti correlati.

I dati trattati hanno natura comune ma non è da escludere la possibilità di trattare dati giudiziari.

La struttura di riferimento è rappresentata dal D.S.G.A. e dagli assistenti amministrativi. Sono coadiuvati dal Dirigente scolastico.

A livello informatico vengono utilizzati computer con software gestionale e con programmi di elaborazione testi. La comunicazione telematica avviene nei confronti del MIUR (per ciò che concerne i flussi finanziari). Solo dati comuni

Titolo II
Trattamento dati con finalità gestionali

Art.12
Gestione finanziaria e gestione del Programma annuale

Di particolare interesse è il trattamento dei dati finalizzato alla gestione finanziaria ed alla gestione del programma. In tale categoria rientra soprattutto il bilancio, la sua predisposizione, esecuzione, ecc. Da considerare anche i rapporti eventualmente intercorrenti con le banche.

I datti trattatati hanno natura comune.

Per ciò che concerne la struttura di riferimento occorre distinguere tra la gestione prettamente contabile e quella amministrativa alla stessa correlata. Se, infatti, per entrambe le gestioni la struttura di riferimento è individuata nel D.S.G.A e nella Segreteria, per quanto riguarda le strutture che concorrono è necessario distinguere: a) per la gestione contabile rileva il dirigente scolastico; b) per la gestione amministrativa rileva il dirigente scolastico ed il corpo docente, rectius, i docenti responsabili di progetto.

A livello informatico vengono utilizzati computer con software gestionale e con programmi di elaborazione testi. La comunicazione telematica avviene nei confronti del MIUR (per ciò che concerne i flussi finanziari). Solo dati comuni.

Art.13
Gestione istituzionale

Il trattamento dei dati qui evidenziato si riferisce alla gestione istituzionale ossia alla gestione di tutti gli atti amministrativi siano essi formati o solo utilizzati dalla scuola.

In particolare rileva la gestione della posta in arrivo ed in partenza mediante l'utilizzo del protocollo informatico dei documenti. E pertanto importante è l'eventuale redazione con "word processor" di documenti in uscita soprattutto quando ciò riguardi documenti riservati. Allo stesso modo rileva la protocollazione riservata di documenti di particolare natura (si pensi a documenti contenenti dati sensibili o giudiziari).

I dati trattatati hanno natura comune ma non è da escludere la possibilità di trattare dati sensibili, con particolare attenzione ai dati concernenti lo stato di salute, nonché dati giudiziari.

La struttura di riferimento è rappresentata dal D.S.G.A. e dalla segreteria. Sono coadiuvati dal Dirigente scolastico.

A livello informatico vengono utilizzati computer con software gestionale e con programmi di elaborazione testi. Non sono previste al momento comunicazioni telematiche.

Art.14
Marcatempo elettronico

Nel IX° circolo didattico Japigia I è in funzione il marcatempo elettronico. Con il quale si effettua la rilevazione dei dati del personale con finalità retributiva.

I dati rilevati hanno natura comune e la struttura di riferimento è la segreteria, coadiuvata dal Dirigente scolastico, dai collaboratori del Dirigente e dal D.S.G.A..

Art.15
Gestione del sito Web della scuola

In questo Istituto è presente il sito Web. La gestione del sito Web acquista rilevanza laddove vengano utilizzati i dati personali degli alunni. In tale circostanza la struttura di riferimento è rappresentata dal corpo docente, coadiuvato dal Dirigente scolastico, ed i dati trattatati sono, di regola, di natura comune. Non è da escludere l'utilizzo di dati sensibili ma ciò può accadere solo dopo una compiuta regolamentazione normativa da parte, ad esempio, del MIUR al fine di risolvere la problematiche concernenti la diffusione dei dati con particolare riferimento a quelli di natura sensibile (occorre ricordare che il codice sulla privacy vieta in modo assoluto la diffusione di dati relativi allo stato di salute). Diversamente solo il consenso dei genitori interessati può sollevare la scuola da responsabilità.

Diversamente la gestione di un sito Web con finalità di comunicazione istituzionale e di propaganda, utilizzando solo dati neutri, non solleva particolari problematiche e la struttura di riferimento può essere individuata nel Dirigente scolastico.

SEZIONE III

Compiti e responsabilità

Art.16

Struttura organizzativa

Negli articoli che seguono si darà conto della suddivisione dei compiti e delle responsabilità tra le diverse unità organizzative in cui si articola la scuola con riferimento al trattamento che ciascuna unità può effettuare. Inoltre vengono evidenziate, alla fine della Sezione, i compiti e le responsabilità del "Responsabile del trattamento dei dati personali", figura espressamente individuata dal codice sulla privacy.

Le unità organizzative sono le seguenti:

1) Dirigente scolastico;
2) Collaboratori del Dirigente scolastico;
3) D.S.G.A.;
4) Corpo docente;
5) Assistenti amministrativi;
6) Collaboratori scolastici e personale ausiliario;
7) Membri degli organi collegiali;
8) Responsabile del trattamento dei dati personali.

Art.17

Il Dirigente scolastico

Il Dirigente scolastico, rappresentante legale della scuola, ha quale compito primario la direzione generale di tutte le attività concernenti l'utilizzo dei dati personali ed è pertanto responsabile, sotto questo profilo, per il trattamento di tutti i dati utilizzati dalla scuola: dati degli alunni con finalità didattico e amministrativa; dati del personale dipendente della scuola; dati del personale esterno utilizzato per collaborazioni professionali; dati dei fornitori di beni e servizi; dati relativi alla gestione finanziaria della scuola; ecc..

In particolare, tra le banche dati di natura cartacea o informatica, poste sotto il suo diretto controllo possono elencarsi: il protocollo riservato, raccolta di documentazione concernente lo stato di salute con particolare riferimento a situazioni di handicap psico-fisico, verbali degli organi collegiali, fascicoli del personale direttivo e del personale docente, ecc.

Il Dirigente scolastico non trasmette dati personali all'esterno.

Art.18
Collaboratori del Dirigente scolastico

I collaboratori del Dirigente scolastico coadiuvano questo ultimo nell'espletamento dei propri compiti sostituendolo in caso di assenza. Sono destinatari di deleghe parziali.

Pertanto anch'essi, nei limiti dei compiti ad essi attribuiti, sono responsabili per il trattamento di tutti i dati utilizzati dalla scuola. Non effettuano comunicazioni all'esterno della struttura.

Art.19
Il D.S.G.A.

Il D.S.G.A. è il responsabile della gestione amministrativa di tutte le pratiche con particolare riferimento a quelle che richiedono la produzione di una risposta o di una certificazione mediante l'utilizzo di programmi di elaborazione testi o di appositi software.

Dirige l'attività del personale di segreteria per ciò che concerne il trattamento di dati personali mediante l'utilizzo di strumenti elettronici ed informatici.

Svolge,infine, attività di supporto al Dirigente scolastico ed al corpo docente.

Sono esclusi dalla sua responsabilità i dati degli alunni trattati per finalità didattica.

Le banche dati cui ha accesso il D.S.G.A., sia cartacee che informatiche, sono: documentazione contabile e finanziaria, elenco dei fornitori, contratti, registri delle presenze del personale, fascicoli del personale, fascicoli degli alunni e documentazione didattica per la conservazione, registro degli infortuni, ecc.

Il D.S.G.A. effettua tutte le comunicazioni di dati autorizzate, secondo quanto disposto dal codice sulla privacy, dalle leggi o dai regolamenti. Le comunicazioni si rivolgono nei confronti di enti pubblici quali: MIUR, Ministero dell'Economia, CSA, Uffici scolastici

regionali, INPDAP, INAIL, INPS. I dati comunicati riguardano: gestione stipendi e Trattamento di fine rapporto, adempimenti previdenziali e fiscali, graduatorie, assunzioni e contratti di lavoro.

Da evidenziare che le comunicazioni che riguardano dati sensibili vengono effettuate nei limiti delle autorizzazioni rilasciate dal Garante per la protezione dei dati personali con validità fino al 31 dicembre 2005. Successivamente a tale data sarà necessario l'intervento regolamentare del MIUR.

Art.20
Corpo docente

I compiti del corpo docente riguardano attività integrative e collaterali nel trattamento dei dati degli alunni con finalità didattica, mediante l'utilizzo di computer. I dati possono riguardare anche le famiglie degli alunni.

Le banche dati dei docenti sono costituite da: registri di classe, registro dei verbali del consiglio di classe, documentazione concernente la programmazione didattica, ecc.

Questo Istituto ha provveduto ha individuare la docente Rosangela Dispoto quale punto di riferimento del corpo docente in materia di trattamento dei dati personali degli alunni per finalità didattica. Nel caso in cui ci fosse necessità di comunicare dati all'esterno, ci si atterrà all'art. 24

Non è prevista alcuna comunicazione all'esterno.

Art.21
Assistenti amministrativi

Gli assistenti amministrativi hanno quale compito primario la gestione di tutte le pratiche amministrative, coordinati e diretti dal D.S.G.A.. La responsabilità degli assistenti amministrativi si estende al trattamento di tutti i dati personali effettuati dalla scuola con l'eccezione dei dati degli alunni trattati per finalità didattica e della gestione del sito Web.

Le banche dati cui possono accedere sono le stesse alle quali può accedere il D.S.G.A..

Questo Istituto ha provveduto, inoltre, ad individuare nella sig.ra Loredana Curci la figura di riferimento all'interno della segreteria per tutto ciò che concerne il trattamento dei dati personali effettuato nella gestione degli affari amministrativi.

Effettuano comunicazioni all'esterno negli stessi termini già visti per il D.S.G.A. Nei confronti di enti pubblici quali: MIUR, Ministero dell'Economia, CSA, Uffici scolastici regionali, INPDAP, INAIL, INPS. I dati comunicati riguardano: gestione stipendi e Trattamento di fine rapporto, adempimenti previdenziali e fiscali, graduatorie, assunzioni e contratti di lavoro. Le comunicazioni che riguardano dati sensibili vengono effettuate nei limiti delle autorizzazioni rilasciate dal Garante per la protezione dei dati personali con validità fino al 31 dicembre 2005. Successivamente a tale data sarà necessario l'intervento regolamentare del MIUR.

Art.22
Collaboratori scolastici e personale ausiliario

I compiti e le responsabilità dei collaboratori scolastici e del personale ausiliario si riferiscono alla ricezione,trasporto e consegna di supporti informatici nei quali sono contenuti dati personali che non richiedono una particolare protezione.

Anche tra i collaboratori scolastici è stata individuata una figura di riferimento: il sig Pietro Somma.

Da evidenziare che i documenti informatici hanno sempre un corrispettivo cartaceo per cui, in caso di distruzione del dato informatico è sempre possibile risalire al dato originario mediante un documento cartaceo.

Art.23
Componenti degli organi collegiali

Il compito primario dei componenti degli organi collegiali è rappresentato dalla partecipazione a riunioni di natura amministrativa, finanziaria, regolamentare nelle quali vengono utilizzati dati personali ricavati da supporti informatici.

I dati utilizzati hanno natura comune ma non si può escludere l'utilizzo di dati sensibili e giudiziari.

Il collegio, con i suoi componenti, rappresenta la struttura di riferimento ed è coadiuvato dal Dirigente scolastico e dai suoi collaboratori, dal D.S.G.A e dagli assistenti amministrativi, dal corpo docente. La figura di riferimento è rappresentata dalla sig.ra Maria Pia Frisini.

Il collegio non effettua comunicazioni all'esterno.

Art.24
Responsabile del trattamento dei dati personali

Come evidenziato all'inizio del presente documento, il Dirigente scolastico ha provveduto ad individuare nel sig. Lorenzo Lavopa il responsabile del trattamento dei dati personali. Questo, nell'ambito delle proprie competenze, ha i seguenti compiti e responsabilità:

a. predisporre le misure organizzative e comportamentali per garantire la sicurezza dei dati personali;
b. Gestire i back-up e le misure per il ripristino dei dati;
c. Gestire gli archivi;
d. Gestire l'aggiornamento dei programmi informatici, adottare le misure idonee a prevenire virus (e simili);
e. Gestire prudentemente la posta elettronica;
f. Gestire le passwords, le credenziali ed i profili di autorizzazione;
g. Predisporre l'informativa soprattutto per ciò che concerne l'utilizzo di dati sensibili e giudiziari;
h. Avere conoscenza delle regole concernenti il trattamento dei dati mediante comunicazione e diffusione degli stessi.
i. Direzione e controllo di tutto ciò che concerne la sicurezza dei dati personali;
j. Nominare, eventualmente, un custode delle passwords.

I responsabili non possono trasmettere dati all'esterno.

Il Titolare del trattamento informa il Responsabile del trattamento dati delle responsabilità che derivano da tale nomina,in relazione a quanto disposto dalla normativa in vigore.

SEZIONE IV

Rischi cui sono soggetti i dati personali e misure da adottare

Titolo I

Analisi dei rischi

Art.25

Classificazione dei rischi

Dopo aver esaminato i dati personali oggetto di trattamento ed aver individuato compiti e responsabilità delle varie unità organizzative, è necessario analizzare i rischi che gravano sui dati personali e le misure adottate o da adottare per garantirne la sicurezza.

Negli articoli che seguono si procederà, pertanto, ad un'analisi degli eventi che possono interessare i dati personali, o meglio, la loro sicurezza, individuandone il grado di rischio e le possibili conseguenze dannose in caso di realizzazione del rischio medesimo. Al fine di una migliore comprensione si è ritenuto opportuno suddividere i rischi che gravano sulla sicurezza dei dati in tre categorie:

1) rischi che derivano da comportamenti degli operatori della scuola;
2) rischi che derivano da comportamenti di soggetti esterni alla scuola;
3) rischi che dipendono dall'utilizzo di strumenti informatici;
4) rischi che si riferiscono al contesto fisico-ambientale.

Successivamente, nel Titolo II di questa Sezione, si indicheranno le misure adottate o da adottare in relazione a ciascuna categoria di rischio.

Art.26
Rischi che derivano da comportamenti degli operatori della scuola

I comportamenti degli operatori che pregiudicano la sicurezza dei dati possono essere di natura colposa o di natura dolosa.

Tali comportamenti si possono così classificare:

a. comportamenti inadeguati caratterizzati da negligenza, disattenzione, imprudenza, incuria;
b. errori materiali concernenti la sicurezza informatica e la sicurezza fisica dei dati;
c. comportamenti fraudolenti, scorretti, sleali.

I comportamenti di cui alla lett. a) e b) presentano un grado di rischio poco elevato per il livello di responsabilizzazione che contraddistingue gli operatori (si veda la parte relativa alle misure adottate).

Le conseguenze che derivano dalla realizzazione del rischio sono: perdita della riservatezza delle proprie credenziali, accesso non autorizzato al computer e possibilità di intrusioni telematiche. Pertanto può verificarsi una conoscibilità dei dati non autorizzata nonché la perdita e la cancellazione dei dati stessi. In questo ultimo caso le conseguenze negative vengono elisi dalla presenza di una copia cartacea di tutti i dati trattati.

Per ciò che concerne i comportamenti di cui alla lett. c) non è possibile individuare il grado di rischio a causa dell'imprevedibilità del comportamento degli operatori anche se, in base alla conoscenza dei dipendenti, il rischio può essere stimato basso.

In caso di comportamento doloso le conseguenze possono andare dall'utilizzo dei dati personali per fini personali alla distruzione o cancellazione degli stessi dati.

Art.27
Rischi che derivano da comportamenti di soggetti esterni alla scuola

I comportamenti di soggetti esterni alla scuola possono essere suddivisi in due categorie:

a) comportamenti che si concretizzano mediante intrusione nella scuola;

b) comportamenti che si concretizzano mediante attività informatica.

Nella lett. a) rientrano i seguenti comportamenti:

1. accesso non autorizzato all'interno della scuola ed, in particolare, all'interno dei locali ad accesso riservato nei quali sono contenuti archivi o strumenti informatici contenenti dati personali;
2. furto degli strumenti informatici sui quali sono contenuti dati personali o copia degli stessi;
3. furto di passwords e credenziali di autenticazione;
4. distruzione degli strumenti informatici o dei locali nei quali sono situati.

Le possibilità che tali rischi si concretizzino sono poco elevate. Di contro, qualora dovesse verificarsi qualcuno degli eventi appena descritti, le conseguenze possono essere abbastanza rilevanti: sabotaggio degli strumenti informatici, accesso abusivo ai dati e possibilità di copia degli stessi, rallentamento o blocco delle attività, perdita o distruzione dei dati.

I comportamenti di cui alla lett. b) sono i seguenti:

1. accessi telematici esterni non autorizzati;
2. intercettazioni telematica di dati;
3. tecniche di sabotaggio quali spamming, spywere, ecc.;

Rispetto a quelli indicati nella lett. a) tali eventi possono più facilmente realizzarsi per la particolarità delle tecniche adottate dai soggetti esterni (si pensi ad hakers altamente specializzati in campo informatico).

Le conseguenze possono avere diversa gravità: visione indebita di dati personali, blocco o malfunzionamento degli strumenti informatici e conseguentemente dell'attività, cattiva gestione del servizio e-mail con cancellazione o mancata visualizzazione di messaggi utili.

Art.28
Rischi che dipendono dall'utilizzo di strumenti informatici

L'utilizzo di strumenti informatici comporta di per sé alcuni rischi propri di tale categoria di strumenti: malfunzionamento e degrado degli strumenti, malfunzionamento e degrado dei supporti informatici.

Inoltre molti dei rischi connessi all'utilizzo degli strumenti informatici dipendono dal comportamento di soggetti esterni alla scuola, come visto nell'articolo precedente (art.27).

Il rischio che tali eventi si concretizzino è medio e le conseguenze possono essere rilevanti: blocco dell'attività, malfunzionamento o blocco della rete locale della scuola, perdita di dati.

Art.29
Rischi che si riferiscono al contesto fisico - ambientale

Infine vi sono una serie di eventi che riguardano l'aspetto fisico-ambientale della scuola dei quali è, normalmente, impossibile prevederne il grado di rischio.

Tali eventi sono i seguenti:

a) Eventi distruttivi accidentali o naturali;

b) Guasto all'impianto elettrico.

Evidente che le conseguenze in caso di concretizzazione di tali rischi possono essere rilevanti: perdita dei dati, blocco del sistema, distruzione degli strumenti o degli archivi informatici sui quali sono contenuti dati personali.

Titolo II
Misure da adottare o adottate

Art.30
Analisi delle contromisure

Negli articoli che seguono saranno individuate le misure poste in essere o da adottare al fine di prevenire o ridurre la possibilità che i rischi individuati nel Titolo I trovino concreta realizzazione.

Nell'analisi delle misure poste in essere o in programma di essere adottate si cercherà di seguire lo schema indicato nell'analisi dei rischi distinguendo tra:

a) rischi che dipendono da comportamenti di operatori della scuola;

b) rischi che dipendono da comportamenti di soggetti esterni alla scuola;

c) rischi che dipendono dall'utilizzo di strumenti informatici;

d) rischi che si riferiscono al contesto fisico ambientale.

E' pur vero che spesso le misure adottate o da adottare con riferimento ad una determinata categoria di rischio servono a prevenire anche rischi riferibili ad altre categorie. Pertanto tali misure, per completezza, saranno elencate in ciascuna categoria di rischio interessata.

Inoltre occorre precisare che sovente l'attuazione delle misure, dal punto di vista economico, dipende dall'intervento dell'amministrazione locale che rappresenta l'interlocutore della scuola ed, in particolare, per ciò che concerne la sicurezza in materia di privacy, del responsabile del trattamento dei dati personali.

Art.31
Misure relative ai rischi che derivano da comportamenti degli operatori della scuola

La misura idonee a prevenire comportamenti scorretti o negligenti da parte degli operatori della scuola non può che riguardare la formazione delle varie categorie di soggetti incaricati di trattare, a qualsiasi titolo, dati personali. Ciò al fine di responsabilizzare tali soggetti e renderli edotti dell'importanza che riveste, a seguito della promulgazione del codice sulla privacy, la riservatezza dei dati personali trattati per finalità istituzionali.

Tale misura è stata adottata da questo istituto scolastico. Difatti si è provveduto alla formazione di coloro che, a vario titolo, trattano dati personali: sia sotto l'aspetto normativo, sia sotto l'aspetto della sicurezza informatica. In particolare si è provveduto a formare il personale relativamente:

a. alla vigenti disposizioni di legge in materia di dati personali (relativamente agli aspetti che interessano la scuola);
b. ai profili di responsabilità che riguardano ciascun operatore scolastico: responsabile del procedimento, Dirigente scolastico e D.S.G.A., assistenti amministrativi, corpo docente, collaboratori scolastici;
c. alla sicurezza informatica: importanza delle copie di back-up, individuazione ed eliminazione dei virus, gestione dei messaggi di posta elettronica ed individuazione dei messaggi di disturbo.

La formazione assume un aspetto rilevante nella gestione della sicurezza e, pertanto, sarà oggetto di programmazione al fine di fornire un continuo aggiornamento agli operatori della scuola, soprattutto per ciò che concerne l'aspetto relativo alla sicurezza informatica.

Altre misure idonee a prevenire la perdita e la distruzione di dati personali, per comportamenti negligenti o errori materiali, sono le seguenti:

d. Regolare back-up dei dati;
e. Pianificazione delle copie di back-up;
f. Formattazione dei supporti riscrivibili contenenti i back-up obsoleti;
g. Distruzione dei supporti non riscrivibili contenenti i back-up obsoleti;

Art.32
Misure relative ai rischi che derivano da comportamenti di soggetti esterni alla scuola

Le misure esaminate in questo articolo sono numerose e si possono distinguere in misure concernenti la sicurezza materiale degli archivi e dei supporti su cui sono contenuti dati personali e misure concernenti la sicurezza informatica nella gestione e nel trattamento dei dati personali utilizzati dalla scuola.

In particolare occorre sottolineare, relativamente alla sicurezza informatica, che le misure individuate sono finalizzate a prevenire condotte illecite (accesso non autorizzato o distruzione di dati, paralisi dell'attività, ecc.) compiute non solo da soggetti esterni alla scuola ma anche da operatori scolastici privi delle specifiche autorizzazioni.

Relativamente alla sicurezza materiale sono state adottate, in tutti i plessi di cui si compone questo Istituto, le seguenti misure:

a. Sistema di vigilanza;
b. Chiusura a chiave dei locali quando non sono presidiati;
c. Controllo dell'accesso ai locali della scuola;
d. Installazione di sistemi anti-intrusione;
e. Protezione dei locali contro intrusi e atti vandalici.

Per ciò che concerne la sicurezza informatica occorre premettere che i computer sono tutti di recente acquisizione ed in tutti sono stati installati programmi aggiornati (sistemi operativi, antivirus, ecc.).

Sono state adottate le seguenti misure:

a. attribuzione di password individuali per l'accesso ai computer:
b. Creazione di profili di autorizzazione diversificati;
c. Disattivazione password in caso di trasferimento del titolare della stessa;
d. Profilo di autorizzazione che non consente la formattazione del disco rigido;
e. Custodia delle password di accesso in luogo chiuso e sicuro;
f. Distruzione dei supporti non riscrivibili contenenti i back-up obsoleti;
g. Formattazione dei supporti riscrivibili contenenti i back-up obsoleti;
h. Protezione dell'accesso ai supporti utilizzati per il back-up dei dati;
i. Installazione di un filtro anti-spamming;
j. Installazione di un firewall con regolare aggiornamento
k. regolare aggiornamento del software antivirus;
l. Verifica con cadenza semestrale dell'efficacia dei programmi antivirus.

Le passwords sono custodite dal D.S.G.A., responsabile del trattamento dei dati.

Le misure di cui alle lett. i) e j) trovano attuazione relativamente a tutti i computer connessi alla rete pubblica.

La sicurezza dei dati personali sarà maggiormente garantita con l'adozione delle seguenti misure:

a. Divieto di effettuare copie non autorizzate su supporti magnetici;
b. Profilo di autorizzazione specifico per l'accesso ai dati sensibili;

c. Cifratura per proteggere i dati degni di particolare attenzione;
d. Firma elettronica per proteggere i dati importanti;

Art.33
Misure relative ai rischi che dipendono dall'utilizzo di strumenti informatici

In questo articolo si individuano le misure capaci di ridurre i rischi che normalmente si accompagnano all'utilizzo si strumenti elettronici.

Le misure adottate sono le seguenti:

a. Regolare back-up dei dati;
b. Pianificazione delle copie di back-up;
c. Piano di back-up per prevenire il disaster recovering;

d. Manutenzione programmata dei computer (hardware, sistemi oprativi, applicazioni software).

Dovranno, invece, essere adottate le seguenti misure:

a. Uso di contenitori di sicurezza per la Conservazione dei supporti di back-up;
b. Verifica della qualità delle copie di back-up

Art.34
Misure relative ai rischi che si riferiscono al contesto fisico - ambientale

Per ciò che concerne i rischi relativi ad eventi accidentali e naturali, quali incendi, infiltrazioni d'acqua, guasti all'impianto elettrico, vi sono alcune misure che possono prevenire il realizzarsi di tali eventi o, quantomeno, diminuirne le conseguenze negative.

Le misure adottate da questo Istituto sono le seguenti:

a. Disponibilità di estintori ad anidride carbonica;
b. Custodia dei dischi di back-up in locali diversi da quello dei computer;
c. Protezione dei locali contro incendi;
d. Protezioni anti-fulmine contro sovratensioni elettriche;
e. Verifica della congruità dei locali volti a prevenire le infiltrazioni d'acqua;
f. Verifica della congruità dei locali volti a prevenire rischi d'incendio;

Sono allo studio, e dovranno essere adottate (con l'intervento in alcuni casi dell'ente comunale), le seguenti misure:

a. Installazione di un gruppo di continuità (quantomeno per il server posto nell'ufficio di segreteria);
b. Verifica ed eventuale miglioramento della solidità degli infissi e dei locali;
c. Custodia dei dischi back-up in armadio ignifugo e chiuso

Attualmente l'impianto di climatizzazione è presente solo nell'ufficio del Dirigente scolastico e negli uffici di segreteria.

Art.35
Considerazioni conclusive in materia di sicurezza

L'ultima misura di sicurezza concerne l'adozione di un piano per la verifica delle misure di sicurezza adottate all'interno dei singoli settori, con cadenza almeno semestrale.

Infine, poiché l'istituto scolastico si prefigge anche l'obiettivo di incrementare la sicurezza dei dati personali contenuti su supporto cartaceo nonché dei relativi archivi, si è proceduto ad una ricognizione di questi ultimi e si è avuto modo di evidenziare la mancanza di locali idonei per la conservazione degli atti nonché mancanza di idonea suppellettile utile ad una sicura conservazione degli atti .

DICHIARAZIONE FINALE

Il presente Documento, composto di 35 articoli, è stato redatto dal Dirigente scolastico e dal Responsabile del trattamento dei dati personali.

IL DIRIGENTE SCOLASTICO
(Prof.ssa Patrizia ROSSINI)

Il responsabile del trattamento
Sig. Lorenzo Lavopa

Protocollo n. 2954/B32
Data 31/03/2009

Timbro