

DIREZIONE DIDATTICA DEL 5° CIRCOLO DI ALESSANDRIA

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

elaborato in base al Decreto Legislativo 30 giugno 2003 n.196 in “materia di protezione dei dati personali” ed al relativo disciplinare tecnico

sottoposto a revisione a seguito dell’entrata in vigore del Decreto del Ministero della Pubblica Istruzione n. 305 del 07.12.2006

Si richiede l’apposizione del timbro postale per la data certa .

Alessandria 27/03/2009

Il Dirigente Scolastico
(dott.ssa Firmina Bacchiocchi)

Documento unico formato da n. 59 pagine

Alessandria 27/03/2009

Il Dirigente Scolastico
(dott.ssa Firmina Bacchiocchi)

1. Premessa

Scopo di questo documento è stabilire le misure organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza, previsti dal Decreto Legislativo del 30 giugno 2003 n. 196 “Codice in materia di protezione dei dati personali” e del Decreto del Ministero della Pubblica Istruzione n. 305 del 07.12.2006.

In particolare tale piano persegue l'obiettivo di:

- a) minimizzare la probabilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi informatici o cartacei contenenti dati personali;
- b) minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni personali, con particolare riferimento a quelle sensibili.

Il presente documento viene redatto da:

- **Firmina BACCHIOCCHI**, dirigente scolastico del Circolo, in qualità di titolare del trattamento, che lo firma;
- **Ester ISACCO**, direttore dei servizi generali e amministrativi, e **Gastone TIRABOSCO**, insegnante di scuola primaria, in qualità di responsabili del trattamento, i quali provvedono a sottoscriverlo in calce.

2. Normativa di riferimento

Articolo	Norma	Descrizione
Art. 11	D.Lgs. 196/03	modalità di raccolta e requisiti dei dati personali
Art. 15	D.Lgs. 196/03	danni cagionati per effetto del trattamento
Art. 31-36	D.Lgs. 196/03	misure di sicurezza dei dati
Art. 169	D.Lgs. 196/03	omessa adozione di misure minime di sicurezza
Disciplinare Tecnico in materia di Misure Minime di Sicurezza (Allegato B D.Lgs.196/03)		
Tabelle descrittive ai sensi del Decreto del Ministero P. I. n. 305 del 07.12.2006		

3. Definizioni

Per la migliore comprensione del documento si ritiene opportuno riportare le principali, seguenti definizioni di ordine generale, così contraddistinte:

a) definizioni generali

- **"trattamento"**: qualunque operazione o complesso di operazioni, effettuati anche senza 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;

- **"titolare del trattamento dei dati personali"**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- **"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 identificativi"**: i dati personali che permettono l'identificazione diretta dell'interessato;
- **"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 od 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;
- **"responsabile del trattamento dei dati personali"**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- **"incaricati del trattamento dei dati personali"**: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- **"interessato"**: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- **"comunicazione"**: il dare conoscenza dei dati personali a uno o più soggetti diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **"diffusione"**: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **"dato anonimo"**: il dato che in origine, o a seguito di trattamento, non può essere associato a un interessato identificato o identificabile;
- **"blocco"**: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- **"banca dati"**: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- **"Garante"**: l'autorità di cui all'articolo 153, istituita dalla legge 31.12.1996 n. 675.

b) definizioni tecniche

- **“comunicazione elettronica”**: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- **“chiamata”**: la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
- **“reti di comunicazione elettronica”**: i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- **“rete pubblica di comunicazioni”**: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
- **“dati relativi all’ubicazione”**: ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell’apparecchiatura terminale dell’utente di un servizio di comunicazione elettronica accessibile al pubblico;
- **“posta elettronica”**: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell’apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

c) definizioni relative alle misure minime di sicurezza

- **“misure minime”**: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell’art. 31;
- **“strumenti elettronici”**: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- **“autenticazione informatica”**: l’insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell’identità;
- **“credenziali di autenticazione”**: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l’ autenticazione informatica;
- **“parola chiave”**: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

- **“profilo di autorizzazione”**: l’insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- **“sistema di autorizzazione”**: l’insieme degli strumenti e delle procedure che abilitano l’accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

4. Il trattamento dei dati

La legge definisce il trattamento di dati come qualunque operazione o complesso di operazioni svolte con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, registrazione, organizzazione, conservazione, elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione, distruzione di dati.

a) Classificazione

I dati oggetto di raccolta, in funzione dell’analisi dei rischi connessi alla loro gestione, possono essere così classificati:

- **dati anonimi**, ovvero la classe di dati a rischio minimo, per la quale non sono previste particolari misure di sicurezza;
- **dati personali**
 - **semplici**, che indicano elementi di individuazione e riconoscimento a rischio medio;
 - **sensibili**, che indicano elementi di individuazione e riconoscimento ad alto rischio, in modo particolare per quelli di natura **giudiziaria** e **sanitaria**.

b) Natura

Una ricognizione dettagliata e attenta della tipologia dei dati utilizzati dall’istituzione scolastica permette di individuarne la natura, in funzione di una loro classificazione ai fini del rischio insito nel loro trattamento.

Presso il Circolo vengono raccolti e utilizzati dati riguardanti le seguenti informazioni:

- origini razziali ed etniche
- convinzioni religiose, adesione a organismi di carattere religioso
- adesione a sindacati od organizzazioni a carattere sindacale
- stato di salute
- informazioni concernenti procedimenti giudiziari
- codice fiscale e altri numeri di identificazione personale
- nominativo, residenza/domicilio, altri elementi di identificazione personale
- dati relativi alla famiglia e a situazioni personali
- lavoro: occupazione attuale e precedente, reclutamento, tirocinio, carriera...
- attività economiche, commerciali, finanziarie e assicurative
- istruzione e cultura: titoli di studio, pubblicazioni, relazioni.....
- dati sul comportamento
- abitudini di vita: viaggi, spostamenti, esigenze alimentari...

c) Raccolta

La raccolta dei dati può essere effettuata direttamente presso l'interessato o presso terzi, che conferiscono dati relativi a interessati diversi dalla propria persona. In questa fase occorre essenzialmente verificare che la raccolta di dati sia necessaria per lo svolgimento di funzioni

istituzionali, nel rispetto dei limiti di legge o di regolamento. Al momento della raccolta, inoltre, occorre fornire all'interessato, o al terzo presso il quale i dati sono raccolti, una informativa orale o scritta circa le finalità e le modalità del trattamento cui sono destinati i dati.

Il Circolo raccoglie e utilizza dati riguardanti le seguenti categorie di soggetti:

- personale dipendente
- esperti e consulenti esterni
- fornitori, commercianti, artigiani
- scolari e studenti
- familiari dell'interessato

d) Gestione

La gestione dei dati raccolti consiste di due distinte operazioni: quelle statiche di registrazione, conservazione, organizzazione, blocco, cancellazione, distruzione; quelle dinamiche di elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione. E' in tale ultima fattispecie che si corrono i maggiori rischi e proprio in quest'ottica si spiegano i diritti che la legge riconosce in capo all'interessato.

Nel Circolo, i dati raccolti vengono trattati con i seguenti strumenti/modalità:

- elaborazione per via telematica
- registrazione ed elaborazione su supporto cartaceo
- registrazione ed elaborazione su supporto magnetico
- organizzazione degli archivi in forma automatizzata
- organizzazione degli archivi in forma non automatizzata
- elaborazione di dati raccolti da terzi
- trattamenti temporanei finalizzati a un'aggregazione dei dati in forma anonima
- predisposizione di informative relativi a inizi o sospetti di frode o truffa
- creazione di profili professionali o relativi a candidati
- creazione di profili relativi a clienti e fornitori
- creazione di altri profili

e) Comunicazione e diffusione

L'output consiste di due distinte operazioni: la comunicazione a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione; la diffusione, ossia il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. In proposito, la legge prevede che la comunicazione o diffusione di dati sensibili da parte di un soggetto pubblico a terzi non istituzionalmente previsti avvenga solo per espressa previsione normativa. In caso contrario, occorre acquisire il consenso scritto dell'interessato.

Il Circolo non diffonde dati, al di fuori delle sue finalità istituzionali, se non in forma anonima. Comunica invece dati, sempre per fini istituzionali o in forza di disposizioni normative, ai seguenti soggetti:

- organi costituzionali o di rilievo costituzionale
- organismi sanitari
- istituti e scuole di ogni ordine e grado
- enti previdenziali e assistenziali
- forze di polizia
- uffici giudiziari
- enti locali e loro associazioni
- enti pubblici

- organizzazioni sindacali e patronati
- banche e istituti di credito
- intermediari finanziari
- imprese di assicurazione
- associazioni e fondazioni
- familiari dell'interessato

5. Analisi del rischio

I rischi a cui sono sottoposti gli archivi presenti nella scuola si possono suddividere in rischi fisici e logici. Alla prima tipologia appartengono tutti gli archivi a supporto cartaceo e in parte quelli su supporto informatico. Alla seconda tipologia appartengono quelli che utilizzano elaboratori elettronici ed in specie quelli connessi in rete, sia locale che geografica.

a) Rischio fisico

Gli archivi cartacei sono conservati, di norma, in armadi con chiave. I rischi fisici a cui sono soggetti sono i seguenti:

- accesso agli uffici e agli archivi di persone esterne all'ente;
- smarrimento per incuria da parte del personale;
- furto, visura e/o copiatura da parte di personale non autorizzato;
- perdita parziale o totale a causa di incendi, allagamenti o per il degrado naturale del supporto;
- atti di vandalismo.

Gli archivi informatizzati risiedono su elaboratori elettronici. I rischi fisici a cui sono soggetti sono i seguenti:

- distruzione dell'elaboratore o dei supporti fisici di backup per eventi esterni;
- guasti hardware dell'elaboratore o interruzione dei servizi di connessione fisica alla rete;
- furto dell'elaboratore e/o dei supporti di backup dei dati;
- perdita di dati dovuta a imperizia del personale addetto;
- accesso agli elaboratori da parte di personale non autorizzato;
- perdita parziale o totale a causa di incendi, allagamenti o per il degrado naturale del supporto;
- atti di vandalismo.

b) Rischio logico

Il rischio logico si riferisce all'utilizzo di elaboratori per la gestione degli archivi sia di dati comuni che sensibili. I rischi di questo tipo si possono così sintetizzare:

- rischio relativo all'utilizzo da parte di personale, interno o esterno, non autorizzato;
- rischio dovuto a intrusioni nel sistema da parte di hacker a fini dimostrativi o di sabotaggio;
- rischio di scaricamento virus e/o trojan per mezzo di posta elettronica e/o operazioni di download eseguite tramite il browser.
- rischi interni ed esterni tipici dei servizi di rete.

• **Misure minime di sicurezza adottate**

Le misure minime di sicurezza adottate riguardano i seguenti aspetti:

a) accessi fisici

Sono definite aree ad accesso controllato quei locali che contengono apparecchiature informatiche critiche e archivi informatici e/o cartacei contenenti dati sensibili. Nel Circolo esse sono così identificate:

- uffici di Segreteria e di Direzione;
- laboratori informatici e didattici della sede centrale e di quelle periferiche;
- locali di archivio e custodia dei documenti della sede centrale e di quelle periferiche.

Tali aree sono soggette alle seguenti regole di gestione:

- durante gli orari di apertura, il pubblico e gli addetti hanno libero accesso ai locali, sotto il controllo e la vigilanza del personale in servizio ad essi preposto;
- al di fuori degli orari di apertura, l'accesso è consentito soltanto in presenza e col consenso delle persone autorizzate;
- di norma, esse sono individuate e designate sulla base delle funzioni svolte;
- eventuali deroghe potranno dar luogo a provvedimenti autorizzativi specifici, per compiti particolari da svolgersi in tempi circoscritti;
- in assenza degli autorizzati, i locali devono essere chiusi e presidiati dal personale collaboratore scolastico responsabile del piano. Tale personale è inoltre responsabile del ricevimento della corrispondenza e della sua collocazione nei locali controllati.

Nello specifico, oltre al dirigente scolastico, al vicario designato e al direttore amministrativo, che hanno accesso universale, le persone autorizzate sono:

Direzione Didattica	Segreteria e Direzione Laboratorio informatico Archivio generale	Amministrazione Amministrazione Amministrazione	u. o. Segreteria
Infanzia "A. Sabin"	Segreteria	Documenti alunni	u. o. Segreteria Responsabile plesso
Primaria "A. Ferrero"	Segreteria Laboratorio informatico	Documenti alunni Didattica alunni	u. o. Segreteria Responsabile plesso Web master Responsabile laboratorio
Primaria "C. Zanzi"	Sala documentazione Laboratorio informatico	Documenti alunni Didattica alunni	u. o. Segreteria Responsabile plesso Coord. Psicopedagogico Web master Responsabile laboratorio
Primaria San Michele	Laboratorio informatico	Documenti alunni Didattica alunni	u. o. Segreteria Web master Responsabile plesso Responsabile laboratorio
Scuole Castelletto M.to	Laboratorio informatico	Documenti alunni Didattica alunni	u. o. Segreteria Web master Responsabili plessi Responsabile laboratorio

I nominativi del personale delle u.o. sono indicati in apposito elenchi suddivisi per u.o.

b) archivi cartacei

Di norma, tutti gli archivi cartacei devono essere collocati in idonei contenitori, muniti di chiavi. Al personale preposto è consentito l'accesso ai soli dati necessari allo svolgimento delle proprie mansioni, per i quali è prevista la restituzione degli atti e dei documenti alla conclusione delle operazioni. Le pratiche in transito, in sospeso o in lavorazione, devono essere custodite a cura del preposto a cui sono affidate. È comunque vietato trattenerle in collocazioni accessibili ad estranei, al di fuori del proprio orario di lavoro.

I docenti sono responsabili della custodia dei registri e dei documenti riguardanti gli alunni, che sono stati loro affidati all'inizio dell'anno scolastico.

c) archivi informatici

Gli archivi informatici del Circolo sono ubicati, essenzialmente, nel laboratorio adiacente l'ufficio di segreteria, dotato di porta blindata e con accesso controllato. Le chiavi sono custodite, in copia, dal dirigente scolastico, dal direttore amministrativo e dal collaboratore scolastico responsabile del piano.

L'accesso alle banche dati e ai programmi di gestione avviene per mezzo di user-id e password personale. Essi sono assegnati in maniera univoca dal responsabile per il trattamento, che assegna inoltre le aree di competenza. La rete della scuola "Ferrero" è inoltre protetta da firewall.

Le operazioni di salvataggio avvengono tramite back up disposto dal responsabile su periferiche removibili conservate in segreteria. Eventuali salvataggi, effettuati dai singoli addetti per mezzo di altri removibili, ricadono sotto la loro diretta responsabilità e devono essere conservati in luoghi decentrati rispetto al posto di lavoro informatico.

6. Incarichi e responsabilità

a) Titolare

Il titolare del trattamento è la scuola e la titolarità è esercitata dal dirigente scolastico.

Nella fattispecie e al momento della stesura del presente documento, il titolare del trattamento è individuato nella persona del dirigente scolastico pro tempore **Firmina Bacchiocchi**.

b) Responsabili

Il comma 3 dell'art. 29 del D. Lgs. 196/2003 consente al titolare di nominare un responsabile del trattamento. Tale figura deve procedere al trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche attraverso periodiche verifiche, esercita la vigilanza su quanto previsto nelle proprie istruzioni.

La scuola si basa su due fondamenti organizzativi: l'attività amministrativa e quella didattica. Pertanto, vagliato il D. Lgs. 196/2003 e valutata la situazione dell'istituzione a cui è preposto, il titolare ritiene necessario e opportuno procedere alla nomina di un responsabile del trattamento per ognuna delle due aree individuate:

- **area amministrativa**

Il profilo del responsabile per l'area amministrativa corrisponde a quello del Direttore dei servizi generali e amministrativi. Tale scelta consente, infatti, di avvalersi di una figura in posizione organizzativa di carattere sovraordinato e, quindi, particolarmente qualificata al compito.

Nella fattispecie e al momento della stesura del presente documento, il responsabile del trattamento per l'area amministrativa è individuato nella persona del direttore pro tempore dei servizi generali e amministrativi **Ester Isacco**. A Lei viene attribuito l'incarico di sovrintendere alla gestione del trattamento dei dati amministrativi, comprensivi degli archivi cartacei e della rete informatica dell'ufficio di Segreteria.

- **area didattica**

Il profilo del responsabile per l'area didattica corrisponde a quello del web master del

Circolo. Tale scelta consente, infatti, di avvalersi di una figura con competenze didattiche unite a particolari competenze informatiche e, quindi, particolarmente qualificata al compito.

Nella fattispecie e al momento della stesura del presente documento, il responsabile del trattamento per l'area didattica è individuato nella persona dell'insegnante di scuola primaria e web master del Circolo **Gastone Tirabosco**. A lui viene attribuito l'incarico di sovrintendere alla gestione del trattamento dei dati didattici, con particolare riferimento ai laboratori informatici utilizzati dai docenti e dagli alunni del Circolo.

Con provvedimento di nomina a parte, tali incarichi vengono definiti nel dettaglio dei compiti che qui di seguito sono riportati in sintesi:

- verifica della liceità e della correttezza nel trattamento dei dati;
- gestione delle reti informatiche e custodia delle password;
- promozione, realizzazione e mantenimento di adeguati programmi di sicurezza;
- promozione e svolgimento di un programma di addestramento e di controllo.

c) Consulenza informatica

La tecnologia progredisce in tempi rapidi. Quella del settore informatico, in tempi rapidissimi. Ciò comporta la necessità di poter contare su consolidate competenze di base, continuamente aggiornate anche mediante il ricorso ad una molteplicità di esperienze dirette. Tale considerazione ha indotto il titolare del trattamento a conferire un incarico di consulenza per la sicurezza informatica, consentendo all'istituzione di avvalersi di una figura particolarmente adeguata e qualificata al compito.

Nella fattispecie e al momento della stesura del presente documento, il consulente per la sicurezza informatica del Circolo è individuato nella persona dell'ingegner **Marcello Gilardenghi**, professore presso l'ITIS "Sobrero" di Casale M.to e realizzatore delle reti del Circolo. A lui compete l'allestimento relativo alle difese anti-intrusione, definito nel dettaglio del relativo provvedimento di nomina.

d) Incaricati

Si definiscono incaricati del trattamento dei dati personali le persone fisiche autorizzate a compiere operazioni di trattamento dei dati personali, mediante incarico conferito dal titolare o dal responsabile. Poiché il Circolo presenta una dimensione organizzativa complessa, in ragione dell'articolazione in funzioni, in servizi e per territorio, il titolare ha ritenuto opportuno suddividerla per **unità organizzative** omogenee, a ciascuna delle quali conferire incarichi distinti per tipologia e per finalità.

Le unità organizzative così individuate sono 5:

1. Unità organizzativa "Segreteria"

In essa rientra tutto il personale che svolge mansioni di ufficio, a qualunque titolo e per qualsiasi periodo. Nella fattispecie e al momento della stesura del presente documento, all'unità organizzativa "Segreteria" appartengono gli assistenti amministrativi in servizio nel Circolo e l'insegnante fuori ruolo, assegnata a compiti amministrativi;

2. Unità organizzativa "Collaboratori"

In essa rientra tutto il personale docente e non docente che collabora alla conduzione del Circolo. Nella fattispecie e al momento della stesura del presente documento, all'unità organizzativa "Collaboratori" appartengono i componenti lo staff di Direzione e i referenti dei progetti di Circolo;

3. Unità organizzativa "Docenti"

In essa rientra tutto il personale che svolge funzioni di docenza nel Circolo. Nella fattispecie e al momento della stesura del presente documento, all'unità organizzativa "Docenti" appartengono

gli insegnanti di ruolo e non di ruolo in servizio nel Circolo, nonché tutti coloro che, anche sporadicamente, intervengono nella conduzione delle attività didattiche svolte;

4. Unità organizzativa “Ausiliari”

In essa rientra tutto il personale che svolge funzioni ausiliarie nel Circolo. Nella fattispecie e al momento della stesura del presente documento, all'unità organizzativa “Ausiliari” appartengono tutti i collaboratori scolastici di ruolo e non di ruolo in servizio nel Circolo, nonché tutti coloro che, anche sporadicamente, intervengono nella conduzione delle attività con funzioni di supporto;

5. Unità organizzativa “Organi Collegiali”

In essa rientrano tutti i componenti eletti o designati negli Organi Collegiali del Circolo. Nella fattispecie e al momento della stesura del presente documento, all'unità organizzativa “Organi Collegiali” appartengono i componenti del Consiglio e della Giunta, i componenti dei Comitati di Valutazione, della Commissione Elettorale e dei Seggi che periodicamente vengono costituiti nel Circolo per procedere alle elezioni scolastiche.

Per ognuna di queste unità, si è proceduto a indicare il dettaglio degli incarichi, mediante provvedimento di nomina accluso a parte.

7. Incidente informatico

Un incidente può essere definito come un evento che produce effetti negativi sulle operazioni del sistema e che si configura come frode, danno, abuso, compromissione dell'informazione, perdita di beni. In caso di incidente informatico, è opportuno procedere a isolare il sistema compromesso dalla rete e spegnerlo correttamente. La successiva fase di indagine e di ripristino del sistema deve essere condotta da personale esperto. Il dirigente scolastico, sentiti i responsabili incaricati, valuterà se informare del caso le autorità competenti, sollecitando altresì le necessarie garanzie di assistenza e di tutela.

8. Formazione

Il buon funzionamento di un piano di sicurezza si realizza attraverso il coinvolgimento di tutto il personale della scuola, creando la cultura necessaria a garantire e a preservare l'integrità e la riservatezza dell'intero patrimonio informativo.

La formazione deve coinvolgere tutto il personale in maniera sistematica e ricorrente. Essa s'intende sviluppata attraverso le seguenti fasi:

- informazione preliminare generalizzata, rivolta a tutto il personale, attraverso la realizzazione di un'apposita iniziativa formativa;
- informazione specifica differenziata, rivolta al personale suddiviso per qualifiche e compiti relativi;
- informazione sintetica, da utilizzare nei riguardi di famiglie, collaboratori, componenti gli OO. CC. , nonché per accompagnare l'inserimento di personale nuovo assunto, o trasferito.

9. Aggiornamento del piano

Il presente piano è soggetto a revisione ogni qualvolta si verificano modifiche all'assetto organizzativo della scuola e in particolare del sistema informativo, oppure danneggiamento o attacchi al patrimonio informativo tali da dover correggere e aggiornare i livelli minimi di sicurezza previsti in sede di analisi del rischio.

10. Accesso a Internet

Il curriculum scolastico prevede che gli alunni, durante la loro attività, imparino i primi approcci alle tecnologie multimediali. Queste, e Internet in particolare, offrono una vasta gamma di risorse diverse per lo svolgimento delle attività didattiche e per una migliore fruizione del tempo

libero. Per alunni e insegnanti la fruizione di Internet è un'opportunità. Essa, però, può costituire anche un pericolo perché esiste la possibilità che in rete si trovi materiale inadeguato, illegale e pericoloso. Per questo motivo il Circolo ha inteso assumere alcune precauzioni, limitandone l'accesso con le indicazioni che si allegano di seguito.

ACCESSO A INTERNET

1. Accertamento dei rischi e valutazione dei contenuti

Il Circolo si fa carico di tutte le prestazioni necessarie per garantire agli alunni l'accesso a materiale appropriato, anche se non è possibile evitare che nessi trovino materiale indesiderato navigando su un computer della scuola.

Gli alunni imparano a utilizzare internet e i motori di ricerca a ricevere e inviare messaggi e-mail tramite caselle di posta elettronica controllate dai docenti. Essi devono essere educati a riconoscere e ad evitare gli aspetti negativi di Internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori. Soprattutto i minori non devono essere sottoposti a materiale di questo tipo e, qualora ne venissero a contatto, devono sempre riferire l'indirizzo Internet all'insegnante o ai genitori.

2. Strategie della scuola per garantire la sicurezza delle tecnologie informatiche e multimediali.

Il Circolo predispone i seguenti accorgimenti:

- utilizzo di firewall per impedire l'accesso dall'esterno ai computer della scuola;
- uso di sistemi operativi che permettono un'efficace gestione della multiutenza;
- l'utilizzo dei laboratori di informatica è regolamentato da un apposito orario settimanale e comunque gli alunni possono accedervi solo se accompagnati dai docenti;
- i sistemi vengono regolarmente controllati, per prevenire ed eventualmente rimediare a possibili disfunzioni dell'hardware e/o del software;
- i responsabili di rete e di laboratorio controllano regolarmente i file utilizzati, i file temporanei e i siti visitati, vigilando affinché i docenti eliminino i percorsi di navigazione dalla Cronologia, se non ne è previsto un loro utilizzo con gli alunni;
- è vietato inserire file sul server o scaricare software non autorizzati da Internet;
- la LAN scolastica è provvista di un software antivirus di rete, aggiornato settimanalmente dal responsabile;
- per utilizzare periferiche personali è necessario sottoporle preventivamente al controllo antivirus;
- utilità di sistema e fili eseguibili, reperibili su supporti provenienti da riviste o altro, non possono essere utilizzati senza autorizzazione;
- di norma, il software utilizzabile è solamente quello autorizzato dalla scuola, regolarmente licenziato e/o open source;
- il materiale presente sullo spazio web dedicato alle attività didattiche della scuola è periodicamente controllato dal responsabile di rete.

3. Norme e linee guida

Tutti gli utenti connessi a Internet

- La legislazione vigente applicata anche alla comunicazione su Internet
- La netiquette (etica e norme di buon uso dei servizi di rete)

Il sistema di accesso Internet del Circolo prevede l'uso di Java con funzioni di proxy, attivabile esclusivamente dal server tramite password, e quindi intermediario con il compito di controllare la possibilità di collegamento esterno. Esiste poi un firewall per evitare intrusioni dall'esterno e dotare la rete di un'efficace protezione antivirus. Il responsabile di rete controlla periodicamente il sistema di filtraggio.

In caso di violazioni delle regole di politica scolastica, il Circolo ha il diritto di impedire l'accesso dell'utente a Internet per un certo periodo di tempo o in modo permanente. La decisione è assunta anche in considerazione dell'età di cui ha commesso infrazione e dell'entità della medesima.

La scuola riferisce comunque alle autorità competenti ogni ritrovamento di materiale illegale.

4. Fornitore di servizi internet

Durante la frequenza scolastica, gli alunni devono utilizzare soltanto fornitori di servizi e-mail approvati dal Circolo.

L'invio e la ricezione di allegati è soggetto al permesso dell'insegnante.

5. Gestione del sito web della scuola

La redazione editoriale del Circolo gestisce le pagine del sito ed è la sua responsabilità garantire che il loro contenuto sia accurato e appropriato. Il Circolo detiene i diritti d'autore dei documenti che si trovano sul sito o ha richiesto e ottenuto il permesso alla loro pubblicazione da parte dell'autore proprietario.

Le informazioni pubblicate sul sito del Circolo relative a persone da contattare non devono mai includere indirizzi privati o altri dati personali. E' vietata la pubblicazione di dati e materiali contenenti informazioni personali sugli alunni e le loro famiglie, senza preventivo consenso scritto di queste ultime.

6. Servizi on line alle famiglie/utenti esterni

La scuola offre all'interno del proprio sito web tutta una serie di informazioni alle famiglie e agli utenti esterni: orari delle classi, dei docenti, delle strutture; impegni collegiali; calendari scolastici; modulistica, testi in uso, biblioteca docenti.

I servizi offerti devono comunque mai riguardare dati sensibili, ovvero dati personali idonei a rivelare l'origine razziale ed etnica, le condivisioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale.

7. Informare sulla Politica d'uso Accettabile (PUA) della scuola.

Le presenti indicazioni di "Politica d'Uso Accettabile della rete" sono rimesse alla conoscenza di tutto il personale del Circolo. Esso deve essere coinvolto nello sviluppo delle linee guida e nell'applicazione delle istruzioni e delle raccomandazioni sull'uso sicuro di Internet.

In casi di dubbi, ognuno dovrà riferirsi ai responsabili di rete e/o di laboratorio, al fine di evitare ogni possibile malinteso.

Anche i genitori degli alunni vengono informati della PUA della scuola, mediante una comunicazione ufficiale e attraverso il sito web del Circolo. Copia integrale del documento viene rimessa ai rappresentanti dei genitori e a tutti coloro che ne fanno richiesta.

a. Accertamento dei rischi e valutazione dei contenuti

Il Circolo si fa carico di tutte le precauzioni necessarie per garantire agli alunni l'accesso a materiale appropriato, anche se non è possibile evitare che essi trovino materiale indesiderato navigando su un computer della scuola.

Gli alunni imparano a utilizzare Internet e i motori di ricerca; a ricevere e inviare messaggi e-mail tramite caselle di posta elettronica controllate dai docenti. Essi devono essere educati a riconoscere e ad evitare gli aspetti negativi di Internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori. Soprattutto i minori non devono essere sottoposti a materiale di questo tipo e, qualora ne venissero a contatto, devono sempre riferire l'indirizzo Internet all'insegnante o ai genitori.

b. Strategie della scuola per garantire la sicurezza delle tecnologie informatiche e multimediali

Il Circolo predispose i seguenti accorgimenti:

- utilizzo di firewall per impedire l'accesso dall'esterno ai computer della scuola;
- uso di sistemi operativi che permettono un'efficace gestione della multiutenza;
- l'utilizzo dei laboratori di informatica è regolamentato da un apposito orario settimanale e comunque gli alunni possono accedervi solo se accompagnati da docenti;
- i responsabili di rete e di laboratorio controllano regolarmente i file utilizzati, i file temporanei e i siti visitati, vigilando affinché i docenti eliminino i percorsi di navigazione dalla Cronologia, se non ne è previsto un loro utilizzo con gli alunni;
- è vietato inserire file sul server o scaricare software non autorizzati da Internet;
- la LAN scolastica è provvista di un software antivirus di rete, aggiornato automaticamente;
- per utilizzare periferiche personali è necessario sottoporle preventivamente al controllo antivirus;
- utilità di sistema e file eseguibili, reperibili su supporti provenienti da riviste o altro, non possono essere utilizzati senza autorizzazione;
- di norma, il software utilizzabile è solamente quello autorizzato dalla scuola, regolarmente licenziato e/o open source;
- il materiale presente sullo spazio web dedicato alle attività didattiche della scuola è periodicamente controllato dal responsabile di rete.

c. Norme e linee guida

Tutti gli utenti devono rispettare le vigenti norme di accesso e navigazione in Internet, nonché le istruzioni e i divieti contenuti nelle presenti raccomandazioni.

Il sistema di accesso Internet del Circolo prevede l'uso di Jana con funzioni di proxy, attivabile esclusivamente dal server tramite password, e quindi intermediario con il compito di controllare la possibilità di collegamento esterno. Esiste poi un firewall per evitare intrusioni dall'esterno e dotare la rete di un'efficace protezione antivirus. Il responsabile di rete controlla periodicamente il sistema di filtraggio e la sua tenuta.

Dietro specifica richiesta, ad ogni unità di personale docente e non docente in servizio nel Circolo viene rilasciata password per il collegamento Internet e la navigazione web, valida per il laboratorio della sua sede di servizio. Tale password permette la tracciabilità dei percorsi e la rintracciabilità dei responsabili di eventuali violazioni a quanto qui disposto. In tal caso, il Circolo si riserva il diritto d'impedire l'accesso dell'utente a Internet, temporaneamente oppure in modo permanente. La decisione è assunta anche in considerazione dell'età di chi ha commesso l'infrazione e dell'entità della medesima.

La scuola riferisce comunque ogni ritrovamento di materiale illegale alle autorità competenti.

d. Fornitore di servizi internet

Durante la frequenza scolastica, gli alunni devono utilizzare soltanto fornitori di servizi e-mail approvati dal Circolo. L'invio e la ricezione di allegati è soggetto al permesso dell'insegnante.

e. Gestione del sito web della scuola

La redazione editoriale del Circolo gestisce le pagine del sito ed è sua responsabilità garantire che il loro contenuto sia accurato e appropriato. Il Circolo detiene i diritti d'autore dei documenti che si trovano sul sito o ha richiesto e ottenuto il permesso alla loro pubblicazione da parte dell'autore proprietario.

Le informazioni pubblicate sul sito del Circolo relative a persone da contattare non devono mai includere indirizzi privati o altri dati personali. È vietata la pubblicazione di dati e materiali contenenti informazioni personali sugli alunni e le loro famiglie, senza il preventivo consenso scritto di queste ultime.

f. Servizi on line alle famiglie/utenti esterni

La scuola offre all'interno del proprio sito web tutta una serie di informazioni alle famiglie e agli utenti esterni: orari delle classi, dei docenti, delle strutture; impegni collegiali; calendari scolastici; modulistica, testi in uso, biblioteca docenti.

I servizi offerti non devono comunque mai riguardare dati sensibili, ovvero 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 od organizzazioni a carattere religioso, filosofico, politico o sindacale.

g. Informare sulla Politica d'Uso Accettabile (PUA) della scuola

Le presenti indicazioni di "Politica d'Uso Accettabile della rete" sono rimesse alla conoscenza di tutto il personale del Circolo. Esso deve essere coinvolto nell'applicazione delle istruzioni e delle raccomandazioni sull'uso sicuro di Internet. In caso di dubbi, ognuno dovrà riferirsi ai responsabili di rete e/o di laboratorio, al fine di evitare ogni possibile malinteso.

Anche i genitori degli alunni vengono informati della PUA della scuola, mediante comunicazione ufficiale e attraverso il sito web del Circolo. Copia del documento viene rimessa ai rappresentanti dei genitori e a tutti coloro che ne fanno richiesta.

* * * * *

*Il presente documento è stato sottoposto a revisione in data 19 marzo 2009 con l'apporto di:
Ester Isacco direttore sga, responsabile trattamento amministrativo
Gastone Tirabosco web master del Circolo, responsabile trattamento didattico
Marcello Gilardenghi consulente di rete
e ratificato dal Consiglio di Circolo nella sua seduta del .*

Il titolare del trattamento
Dirigente scolastico
(Firmina Bacchiocchi)