



ISTITUTO COMPRENSIVO G. MAZZINI
P.le S. Andrea n. 25/26
58019 PORTO SANTO STEFANO (GR)
Distretto Scolastico n. 37

Prot. 1661/C2

Porto Santo Stefano lì, 19/03/2009

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
REVISIONE anno 2009

Il presente documento è redatto ai sensi dell'art. 34 e 35 del Dlgs 30 Giugno 2003, n. 196, della direttiva 11 Febbraio 2005 del Presidente del Consiglio dei Ministri, del regolamento relativo al trattamento dei dati sensibili e giudiziari del settore dell'istruzione approvato dal MPI con Decreto n. 305 del 7 dicembre 2006 e detta informazioni sulle misure minime di sicurezza in materia di protezione dei dati personali ed inoltre ai sensi del Disciplinare Interno per l'utilizzo dei servizi di Posta elettronica ed accesso ad Internet, erogati dal Sistema Informativo del Ministero della Pubblica Istruzione emanato dal MPI e pubblicato sul Bollettino n. 81 del Marzo 2007 e, successivamente, sulla Gazzetta Ufficiale - Serie generale n. 58 del 10.03.2007.

1 - INFORMAZIONI ESSENZIALI

1.1 - Descrizione sintetica attività

L'Istituto, in qualità di Scuola Statale, a norma delle vigenti disposizioni, svolge attività educativa, didattica e formativa, curriculare ed extracurricolari, di valutazione ed orientamento rivolta ad alunni di Scuola ed altri soggetti.

1.2 - Individuazione dei dati trattati

Nell'ambito di tale attività la Scuola gestisce i dati:

- Del personale per la gestione del rapporto di lavoro, selezione e reclutamento, del contenzioso e dei provvedimenti disciplinari.
- Degli alunni e delle loro famiglie per le attività propedeutiche all'avvio dell'anno scolastico, per l'espletamento della attività educativa, didattica e formativa, di valutazione, per la gestione dei rapporti Scuola-famiglia e del contenzioso.
- Dei componenti degli organi collegiali e commissioni istituzionali
- Dei fornitori per l'acquisto di beni, materiali e servizi necessari per lo svolgimento delle attività indicate al punto 1.1

1.3 - Natura dei dati trattati

Per la individuazione dei dati sensibili e giudiziari trattati dalla Scuola, si fa riferimento alle schede allegare al Decreto n. 305 del 7 dicembre 2006, allegare come parte integrante al presente provvedimento (pagine da 6 a 17 della gazzetta ufficiale n.11 del 15 Gennaio 2007 serie generale n.11).

1.4 - Struttura di Riferimento

I dati sopra indicati vengono gestiti in modo unitario presso la sede centrale dell'Istituto Comprensivo di Porto Santo Stefano.

Alcuni documenti, di natura riservata, sono custoditi in un apposito armadio, chiuso a chiave, sotto la custodia del Dirigente Scolastico.

2 - TRATTAMENTI CON STRUMENTI ELETTRONICI

2.1 - Elenco dei trattamenti di dati personali

Si intendono **dati personali** da salvaguardare tutte le informazioni contenute nel data base del gestionale **Sissi in Rete** utilizzato dall'ufficio di segreteria per la gestione delle seguenti aree:

Area Alunni

Area Personale

Area Nuovo Bilancio

Area Magazzino

Area Protocollo Informatico

Area Retribuzioni

2.2 – Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati.

Sono incaricati del trattamento dei dati delle aree sopraindicate i Sig.ri:

<i>Qualifica</i>	<i>Aree di lavoro trattate</i>
Direttore SGA	Tutte
Assistente Amm.vo	Alunni/SIDI
Assistente Amm.vo	Magazzino/Bilancio/Formazione/Personale/SIDI
Assistente Amm.vo	Personale/Retribuzione/SIDI
Assistente Amm.vo	Personale/SIDI
Assistente Amm.vo	Protocollo/Archivio/Alunni/SIDI

Ciascun incaricato del trattamento dei dati è responsabile delle aree di competenza. Questi devono attenersi alle prescrizioni e indicazioni contenute nelle schede allegate al regolamento approvato dal MPI con Decreto n. 305 del 7 dicembre 2006, ed in particolare per la individuazione:

- delle finalità di rilevante interesse pubblico da perseguire
- dei tipi di dati da trattare
- delle operazioni da eseguire (particolari forme di trattamento)
- delle modalità di raccolta e elaborazione delle informazioni.

2.3 – Analisi dei rischi che incombono sui dati

Sono individuati i seguenti rischi sulla integrità dei dati:

- Intrusione illecita nella base dati di persone non autorizzate
- Furto o guasto della postazione Server
- Calamità naturali

2.4 – Misure adottate per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della custodia e accessibilità.

- **Integrità e disponibilità dei dati**

La integrità e la disponibilità dei dati è garantita da operazioni settimanali di Backup dell'intera base dati. Il processo di Backup avviene mediante copia compressa del **data base**, (comprensivo dei dati di tutte le aree indicate al punto 2.1), su supporto di massa interno e supporto magnetico esterno con periodicità giornaliera e prima della installazione di nuovi aggiornamenti. Il nome del file di backup è diverso per ogni sessione di salvataggio in modo da avere copie della base dati effettuate in date diverse. Il supporto esterno è conservato in cassaforte.

Con periodicità semestrale si eseguono prove di ripristino dei dati (simulazione da distruzione o danneggiamento dati). Di detta operazione viene redatto apposito verbale.

- Accesso alla rete interna e al data base di Sissi in rete.

L'accesso ai computer della rete è protetto dalla richiesta del **nome utente e password**, secondo le specifiche tecniche previste dai sistemi operativi Windows2000 e WindowsXP.

Le password vengono modificate obbligatoriamente con cadenza annuale e ogni qualvolta l'amministratore del sistema lo ritenga necessario.

L'accesso al data base di **Sissi in rete** è consentito esclusivamente alle persone indicate al punto 2.2. ed avviene tramite identificativo (nome utente) e password assegnate a ciascun dipendente dall'amministratore del sistema **in busta chiusa**. Ciascun dipendente ha la facoltà di cambiare in modo autonomo la password di accesso assegnata.

E' fatto divieto ai dipendenti di **accedere al sistema** con il nome utente dei colleghi.

- Protezione delle aree e dei locali rilevanti ai fini della custodia e accessibilità

Le porte di accesso agli uffici sono chiuse a chiave quando non c'è il personale di segreteria. Il servizio di chiusura e apertura degli uffici è garantito dal personale collaboratore scolastico.

- Protezione da virus

Ciascuna postazione, incluso il server, è protetta da un antivirus per reti "Symantec Antivirus corporate edition". L'aggiornamento delle impronte virali avviene giornalmente. E' pianificata la scansione settimanale dei supporti di massa in dotazione alle postazioni in rete.

2.5 – Criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento della base dati.

In presenza di distruzione o danneggiamento della base dati si procede nell'ordine:

- Al ripristino del funzionamento dell' hardware con la sostituzione delle parti non funzionanti.
- Al ripristino dell'ultima copia interna della base dati qualora il danneggiamento non ha riguardato il supporto di massa interno del server.
- Al ripristino dell'ultima copia esterna della base dati negli altri casi.

2.6 – Interventi formativi degli incaricati del trattamento

Al fine di rendere gli incaricati al trattamento dei dati 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 e delle responsabilità che ne derivano, sono organizzati corsi di formazione con cadenza annuale. La formazione è programmata nel periodo Settembre-Dicembre di ciascun anno al fine di consentire la formazione anche del personale che assume servizio il 1° settembre presso l'ufficio. Viene comunque consegnata ai nuovi assunti una informativa per il trattamento dei dati.

3 - TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

3.1 – Aggiornamento dei documenti cartacei

L'aggiornamento dei fascicoli cartacei dei dipendenti e degli allievi è affidato al personale indicato al punto 2.2) ed avviene nel rispetto delle indicazioni fornite dalle schede indicate al punto 1.3).

3.2 – Conservazione e custodia dei documenti cartacei

I documenti cartacei relativi al personale e agli alunni sono conservati in fascicoli personali. Questi sono conservati:

- Presso gli uffici di segreteria per il personale in servizio e gli allievi in frequenza.
- Presso gli archivi dell'ufficio, organizzati in faldoni, per gli atti del personale non più in servizio e degli allievi non più frequentanti.

Tutti i documenti sono conservati in armadi. Le porte di accesso agli archivi sono chiuse a chiave.

3.3 – Accesso ai documenti cartacei

L'accesso ai documenti è consentito esclusivamente al personale individuato al punto 2.2).

4 – LINEE GUIDA PER POSTA ELETTRONICA E INTERNET

4.1 - Principi

Il disciplinare del MPI è stato predisposto nel rispetto della vigente disciplina in materia di Privacy, con riguardo, in particolare, alle norme del D. Lgs. 196/03 (Codice in materia di protezione dei dati personali) che disciplinano il trattamento effettuato dai soggetti pubblici e la Direzione Generale per i Sistemi Informativi garantisce che il trattamento dei dati personali dei dipendenti, effettuato per verificare il corretto utilizzo della Posta elettronica e di Internet, sia conforma ai seguenti principi:

il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (*art. 3 del Codice; par. 5.2 del Provvedimento*);

il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (*art. 11, c. 1, lett. a), del Codice*) poiché le tecnologie dell'informazione, in modo più marcato rispetto ad apparecchiature tradizionali, permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa, anche all'insaputa o, comunque, senza la piena consapevolezza dei lavoratori (*par. 3 del Provvedimento*);

principio di *pertinenza e non eccedenza* (*par. 6 del Provvedimento*), in virtù del quale:

- a) i trattamenti devono essere effettuati per finalità *determinate, esplicite e legittime* (*art. 11, c. 1, lett. b) del Codice; par. 4 e 5 del Provvedimento*);
- b) il personale deve trattare i dati “*nella misura meno invasiva possibile*”;
- c) le attività di monitoraggio devono essere svolte solo da soggetti preposti (*par. 8 del Provvedimento*) ed essere “*mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza*” (*Parere n. 8/2001, punti 5 e 12*).

4.2 - Informativa sulle modalità di utilizzo di Posta elettronica ed Internet

Questa Istituzione Scolastica, aderendo al Disciplinare dell'Amministrazione Centrale, comunica le seguenti informazioni, raccomandazioni e indicazioni sulla modalità di utilizzo della posta elettronica e di internet:

- a) È essenziale che ciascun utente della rete riconosca le responsabilità insite nel fatto di avere accesso a un gran numero di servizi, siti, sistemi e persone.
- b) È l'utente, in ultima analisi, ad essere responsabile delle proprie azioni quando accede ai servizi di rete.
- c) “Internet” o “La Rete” non è una rete sola; piuttosto, è un insieme di migliaia di reti singole che hanno scelto di permettere che il traffico di altre reti le attraversi. Il traffico inviato su Internet potrebbe attraversare un certo numero di reti differenti prima di raggiungere la propria destinazione. Pertanto, gli

utenti coinvolti in questo *internetwork* devono essere consapevoli del carico che possono imporre, implicitamente, su tutte le reti collegate, anche al di fuori della propria.

d) L'uso della rete è un privilegio, non un diritto, e, come tale, potrebbe essere temporaneamente o definitivamente revocato in qualunque momento a causa di una condotta scorretta.

d) Si raccomanda a tutti gli addetti ai servizi della posta elettronica (ed in generale gli utenti che utilizzano connessioni e risorse Internet messe a disposizione dalla Istituzione scolastica, di osservare le linee guida riportate nel documento citato. Si ritiene precisare che la mailbox utilizzate consentono di avere una corrispondenza con utenti esterni alla istituzione scolastica, e che tale corrispondenza risulta essere sempre proveniente dalla scuola. Il rispetto della “netiquette” diventa in questo caso ancor più importante.

e) Gli addetti ai servizi e gli utenti di posta sono invitati ad osservare le seguenti indicazioni:

- Dato il carattere “istituzionale” delle caselle postali Internet della scuola, gli utenti dovrebbero evitare di inoltrare messaggi non direttamente inerenti alle proprie competenze. Inoltre, deve essere prestata attenzione a ciò che viene scritto soprattutto riguardo altre persone o organizzazioni: il messaggio potrebbe essere diffuso e/o citato con facilità.
- L'uso del sistema di posta Internet a scopi personali non è ammesso nella stessa misura in cui non è ammesso l'uso a scopo personale del telefono, del materiale di consumo e di altre risorse della struttura scuola in cui si opera. Allo stesso modo non è ammesso l'uso del sistema di posta della istituzione scolastica (ed in generale di qualsiasi risorsa Internet fornita dalla scuola) per attività commerciali o a scopo di lucro, ed in genere per scopi non previsti dalle norme statutarie della istituzione scolastica.
- Non usare un linguaggio irrispettoso o comunque non apprezzato. Evitare di spedire messaggi provocatori. Evitare di rispondere a messaggi provocatori.
- Non spedire ripetutamente messaggi “a tutti” senza curarsi del fatto che i destinatari siano o meno realmente interessati al vostro messaggio. In generale le liste di distribuzione sono un efficiente strumento di lavoro, ma è necessario usarle con criterio ed evitarne l'abuso.
- Evitare di spedire in allegato files lunghi. Questi, oltre a congestionare la Rete e sovraccaricare i server di posta, potrebbero provocare la saturazione dello spazio disponibile alla casella e problemi a chi utilizza connessioni “lente”. Tenere presente anche che chi riceve la posta dovrà sostenere un costo telefonico proporzionale alla dimensione del messaggio.
- Se un file di grandi dimensioni deve essere spedito ad un limitato numero di destinatari, informare sempre con un breve messaggio il singolo destinatario prima di spedire l'allegato, e dare modo a questi di accettare o rifiutare l'invio del file via posta elettronica.
- Se lo stesso file di grandi dimensioni deve essere inviato a molti utenti, si raccomanda di utilizzare un sito web o ftp per pubblicare tale file e comunicare via posta elettronica agli interessati l'indirizzo (URL) da cui poterli prelevare.
- Se non è possibile evitare di spedire un allegato di grandi dimensioni procedere all'invio solo dopo avere informato il/i destinatario/i. Se esiste il dubbio che il messaggio non sia stato inoltrato correttamente, evitare assolutamente di rispedirlo subito: inviare invece un messaggio ad uno o più destinatari chiedendo una conferma al vostro dubbio.

Nota: Per le RFC1855 un file è "di grandi dimensioni" se supera i 50Kbytes. Orientativamente si raccomanda di non inoltrare files allegati di dimensione superiore a 250Kbyte a più destinatari.

- Per quanto riguarda gli allegati, ed in generale i files scambiati via posta o web/ftp, valgono le stesse indicazioni fornite per il precedente sistema di posta, in particolare per i files Word ed Excel, salvo diverse indicazioni.
- Includere sempre nel campo "soggetto del messaggio" (Subject) un testo pertinente al contenuto del messaggio stesso, in modo che il destinatario possa, se necessario, localizzarlo velocemente.
- Includere sempre la firma in fondo ai messaggi. La *firma* dovrebbe comprendere: nome, cognome, funzione, organizzazione di appartenenza, il vostro indirizzo di posta elettronica, e, opzionalmente, l'indirizzo postale e un recapito telefonico.
- Applicare il buonsenso per capire quanto una informazione che ricevete sia realistica prima di dare per valido un messaggio.
- Il contenuto e la gestione di una mailbox è responsabilità dell'utente incaricato al presidio della stessa. In particolare questi dovrà di norma controllare la posta in arrivo almeno una volta al giorno e, se necessario, smistare correttamente e tempestivamente la posta in entrata.
- Il comportamento "corretto" dell'utente Internet è definito, oltre che dal disciplinare interno e da questo documento, anche dal rispetto dei diritti individuali, dalla cultura e dalla morale sociale, e dal buon senso comune.
- Se vengono riscontrati problemi hardware, software o di sistema, verificare localmente se ci sono persone che possono aiutarvi a risolverli: in caso contrario contattare la Ditta Fans Computer di Porto Santo Stefano.
- Se vengono ricevuti messaggi considerati illegali o non ammessi dalle norme di comportamento generali e le norme contenute in questo documento, rivolgersi al vostro Postmaster.

5 – NOTIFICA E PUBBLICAZIONE DEL PRESENTE DOCUMENTO

5.1 – Notifica agli addetti al trattamento dei dati

Il presente documento è notificato al personale incaricato del trattamento dei dati indicato al punto 2.2).

5.2 – Pubblicazione

Il presente documento è pubblicato all'albo dell'Istituto unitamente alla copia integrale del Decreto del MPI 7 dicembre 2006, n. 305.

IL DIRIGENTE SCOLASTICO
(Prof. Giancarlo STOPPA)