Ministero dell'Istruzione
dell'Università e Ricerca

ISTITUTO COMPRENSIVO STATALE
"SAN GIOVANNI BOSCO"
Via Dante n. 18 – 92028 Naro (AG)
Tel. 0922 956081 – Fax 0922 956041
E-mail agic85300c@istruzione.it - P.E.C. agic85300c@pec.istruzione.it
C.F. 82002930848

Prot. n. 4781/B7 Naro, 18/11/2014

DISPOSITIVO DI DISCIPLINARE INTERNO AI FINI DELLA REGOLAMENTAZIONE SULL'USO DI INTERNET DELLA POSTA ELETTRONICA, DEI TELEFONI E DEI FAX (POLICY DELLA SCUOLA)

1. Premessa

L'uso degli strumenti informatici, della posta elettronica e l'accesso ad Internet da parte delle amministrazioni pubbliche si va' sempre più diffondendo sotto l'impulso della nuova legislazione, con l'obiettivo di migliorare l'efficienza operativa, contenere i costi ed assicurare una maggiore qualità delle prestazioni.

I servizi informativi sono ormai diventati fondamentali anche per gli istituti scolastici che sempre più dovranno utilizzare strumenti come la posta elettronica ed Internet per fornire servizi all'utenza e per migliorare la propria efficienza.

Pertanto è necessario che siano adottate adeguate ed opportune misure di sicurezza volte a proteggere la disponibilità e l'integrità delle risorse informative e a tutelare la riservatezza dei dati personali di tutti. A questo proposito si richiama quanto viene riportato anche nelle Linee Guida per la Sicurezza ICT delle Pubbliche Amministrazioni del CNIPA (Comitato Nazionale per l'Informatica nella Pubblica Amministrazione):

"Tutti i dipendenti dell'Amministrazione sono tenuti ad utilizzare i servizi di rete solo nell'ambito delle proprie mansioni di lavoro, secondo direttive circostanziate, essendo consapevoli che ogni accesso ad Internet può essere facilmente ricondotto alla persona che lo ha effettuato. Occorre quindi che i dipendenti si comportino con il massimo livello di professionalità quando operano in Internet, evitando eventi dannosi, anche al fine di non danneggiare l'immagine dell' Amministrazione".

Dall'esame di diversi reclami, segnalazioni e quesiti pervenuti, il Garante per la protezione dei dati personali ha preso atto dell'esigenza di prescrivere ai datori di lavoro pubblici e privati alcune misure, necessarie o opportune, per conformare alle vigenti disposizioni in materia di Privacy il trattamento di dati personali effettuato per verificare il corretto utilizzo, nel rapporto di lavoro, della Posta elettronica e di Internet.

A tale scopo è stato emanato il provvedimento generale pubblicato sul Bollettino n. 81 del Marzo 2007 e, successivamente, sulla Gazzetta Ufficiale – Serie generale n. 58 del 10.03.2007 (di seguito "il Provvedimento").

Con il presente disciplinare si fornisce concreto riscontro alle prescrizioni del Garante e si conforma a quanto previsto nelle conclusioni del Provvedimento, al punto 2), lett. a).

Principi

Il presente disciplinare viene 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.

L'Istituto Scolastico garantisce che il trattamento dei dati personali dei dipendenti, effettuato per verificare il corretto utilizzo della Posta elettronica e di Internet, si conforma ai seguenti principi:

a) 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);
b) 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);
c) principio di pertinenza e non eccedenza (par. 6 del Provvedimento), in virtù del quale:
   - 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);
   - il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile";
   - 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).

2. Informative sulle modalità di utilizzo di Posta elettronica, Intranet ed Internet sul dominio istruzione.it

I servizi di posta elettronica del dominio istruzione.it, quelli forniti dal sito www.istruzione.it e dalla intranet ministeriale sono direttamente gestiti dalla **Direzione Generale per i Sistemi Informativi** che ha diffuso specifiche informative in merito alle modalità di utilizzo dei suddetti servizi. Per agevolare la presa visione di tali informative da parte di tutto il personale riportiamo di seguito i relativi riferimenti.

Posta elettronica

Le politiche di uso della Posta elettronica del dominio istruzione.it sono articolate in due documenti in funzione della tipologia di utente:

- [1] utilizzo del servizio di Posta elettronica per gli utenti "standard" (docenti, dirigenti scolastici, personale ATA)
- [2] utilizzo del servizio di Posta elettronica per gli utenti del Sistema Informativo dell'Istruzione (personale dell'amministrazione centrale e periferica, istituzioni scolastiche).

Di seguito si riporta la denominazione dei relativi documenti e l'indirizzo a cui sono reperibili:

	Nome documento	**Indirizzo Intranet**	**Indirizzo Internet**
[1]	politica_pel_standard_v6.pdf	http://www.mpi.it/argomenti/sicurezza_informatica/default.htm	http://www.pubblica.istruzione.it/webmail/manuali/politica_pel_standard_v6.

			pdf
[2]	politica_pel_sidi_v6.pdf	http://www.mpi.it/argomenti/sicurezza_informatica/default.htm	http://www.pubblica.istruzione.it/webmail/manuali/politica_pel_sidi_v6.pdf

Internet

Le politiche di utilizzo del servizio di accesso alla rete Internet [3] si riferiscono solo al personale dell'Amministrazione centrale e periferica e sono disponibili sul sito Intranet. Di seguito si riporta la denominazione del relativo documento e l'indirizzo a cui questo è reperibile:

	Nome documento	**Indirizzo Intranet**	**Indirizzo Internet**
[3]	politica_internet_sidi_v4.pdf	http://www.mpi.it/argomenti/sicurezza_informatica/default.htm	Non Disponibile

Politica di utilizzo delle postazioni di lavoro

La Direzione Generale per i Sistemi Informativi ha provveduto a pubblicare sul sito Intranet il documento relativo alle politiche di utilizzo delle postazioni di lavoro ed accesso ai sistemi ed ai servizi informatici per gli utenti del Sistema Informativo dell'Istruzione, di cui si riportano di seguito i riferimenti [4]:

	Nome documento	**Indirizzo Intranet**	**Indirizzo Internet**
[4]	politica_PdL_v3.pdf	http://www.mpi.it/argomenti/sicurezza_informatica/default.htm	Non Disponibile

3. Utenti autorizzati all'uso di Internet

Per quanto riguarda l'uso delle dotazioni informatiche e l'accesso ad internet si individuano 4 tipologie di utenti:

1) Personale amministrativo: autorizzato all'uso per lo svolgimento dell'attività amministrativa
2) Personale docente: autorizzato all'uso per qualunque attività educativa, didattica e formativa.
3) Alunni: autorizzato limitatamente all'attività educativa, didattica e formativa programmata dai docenti

4. Misure di tipo organizzativo

5.1 Ubicazione postazioni di lavoro

Per quanto riguarda il personale amministrativo, ogni dipendente riceve indicazione della postazione di lavoro a lui assegnata al momento della presa di servizio, ovvero in caso di cambiamento della propria posizione. L'uso di tale postazione non è tuttavia da ritenersi esclusivo e ciascun dipendente a seconda delle necessità potrà operare su altro PC non direttamente assegnato ***usando sempre la propria credenziale di accesso personale*** (nome utente e password).

L'accesso ad Internet da parte del personale tecnico, docente e degli alunni potrà avvenire nelle classi, nei laboratori ed in qualunque altro luogo a tale attività destinato.

5.2 Sistema di autenticazione

Al fine di ridurre al minimo il rischio di impieghi abusivi, l'accesso alle postazioni destinate all'attività amministrativa è protetto tramite sistema di autenticazione che richiede l'immissione di un apposito codice utente e della relativa password. La gestione degli utenti è fatta in maniera centralizzata sul server di segreteria su cui è configurato un dominio in ambiente Windows server e nel quale potranno quindi essere conservate informazioni relative agli accessi dei singoli utenti.

A causa degli eccessivi costi di gestione, non si è potuto fino ad ora realizzare un analogo sistema di autenticazione centralizzato per la gestione degli utenti relativi all'attività didattica. Per questo motivo, non potendo garantire sulla rete destinata all'attività didattica le misure minime di sicurezza previste dall'allegato b del D.Lgs 196/03, non è autorizzato il trattamento di dati personali sui PC collegati alla rete didattica d'istituto.

5.3 Istruzione e formazione del personale

Il personale ha ricevuto specifiche istruzioni scritte in merito al comportamento da adottare nell'uso delle dotazioni informatiche messe a loro disposizione. In base alla criticità dei trattamenti effettuati da ciascuna componente, sono stati approntati specifici interventi di formazione.

5. Misure di tipo tecnologico connesse all'uso della posta elettronica

Il MIUR mette a disposizione di ogni dipendente una casella personale sul dominio istruzione.it. Rimandando ai documenti citati nel punto 3 del presente regolamento per una visione completa delle politiche di utilizzo adottate dal MIUR, si mettono in evidenza i seguenti punti:

- *E' consentito l'utilizzo del proprio account nel dominio "istruzione.it" a fini privati e personali, purché tale utilizzo non sia causa, diretta o indiretta di disservizi dei sistemi elaborativi e dei servizi di posta elettronica dell'Amministrazione.*
- *Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè, rispettando le leggi, la presente e altre politiche e procedure del Ministero della Pubblica Istruzione e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale*
- *E' fatto divieto a tutti gli utenti di utilizzare il servizio di posta elettronica per inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione del Ministero della Pubblica Istruzione.*
- *E' vietato l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali.*
- *L'Amministrazione registra e conserva, in forma anonima, i dati delle caselle di posta elettronica messe a disposizione dei propri utenti, tramite scrittura in appositi file di log, delle seguenti informazioni minime: mittente del messaggio; destinatario/i; giorno ed ora dell'invio; esito dell'invio.*

Per evitare ogni interferenza con la sfera privata del personale docente e ATA, qualunque comunicazione di interesse amministrativo o di lavoro dovrà avvenire per mezzo delle caselle istituzionali agic85300c@istruzione.it e agic85300c@pec.istruzione.it

La consultazione della posta elettronica da parte dei dipendenti può quindi riguardare:

- caselle personali: su dominio istruzione.it, messa a disposizione da parte del MIUR (e/o casella personale privata, su altro dominio)
- caselle istituzionali di lavoro

UTILIZZO DELLE CASELLE PERSONALI

Il personale può consultare in orario di servizio caselle personali per motivi legati alla propria attività lavorativa. La gestione deve essere effettuata tramite servizi di "webmail": non è consentito configurare su computer dell'Istituto appositi programmi tipo Outlook o Thunderbird per gestire le proprie caselle personali (anche per garantire al dipendente la dovuta riservatezza).

Nell'uso di caselle personali all'interno della scuola, al dipendente non è comunque consentito:

- inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione della Scuola o del MIUR;
- l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali;
- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra lavorative o azioni equivalenti.

UTILIZZO DELLE CASELLE ISTITUZIONALI DI LAVORO

Le caselle istituzionali sono gestite dagli incaricati in base ai compiti loro assegnati. In caso di assenza dell'incaricato abituale, questo potrà essere sostituito da altro personale, in base all'organizzazione interna del lavoro disposta da D.S. o D.S.G.A.: quindi tali caselle devono essere utilizzate solo a scopo lavorativo e NON devono essere utilizzate come caselle personali.

Oltre alle disposizioni impartite per l'utilizzo delle caselle personali, si aggiungono le seguenti disposizioni:

- Evitare di aprire messaggi provenienti da mittenti sconosciuti e che contengono allegati sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd,....). In caso di dubbio consultare un tecnico.
- Nel caso in cui si debba inviare un documento all'esterno dell'Istituto, se non specificamente destinato alla modifica, è preferibile utilizzare il formato *.pdf.
- Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.
- Evitare di inviare allegati di dimensioni eccessive (se necessario usare formati compressi come *.zip, *.rar,...)
- L'iscrizione a "mailing list" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.
- La casella di posta deve essere mantenuta in ordine.

6. Misure di tipo tecnologico connesse all'uso di Internet

L'Istituto Scolastico intende limitare nel maggior grado possibile i controlli sulla navigazione (che potrebbero determinare il trattamento di informazioni personali o sensibili anche non pertinenti l'amministrazione).

Per tale motivo è fondamentale il rispetto delle disposizioni elencate, che hanno il fine di ridurre il rischio di usi impropri della "navigazione".

1. Al personale non è consentito:
   - servirsi o dar modo ad altri di servirsi della stazione di accesso a internet per attività non istituzionali, per attività poste in essere in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
   - utilizzare sistemi Peer to Peer (P2P), di file sharing, podcasting, webcasting social network o similari (salvo specifiche attività espressamente autorizzate per le finalità istituzionali).
   - Utilizzare sistemi Social Network quali twitter, face book, etc.
2. Ogni utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico mediante virus o mediante ogni altro software aggressivo (attenzione nell'aprire mail e relativi allegati, non navigare su siti poco professionali, ecc..)
3. Ogni utente è tenuto a controllare la presenza e il regolare funzionamento del software antivirus, segnalando ogni eventuale problema all'amministratore di sistema.

Si ricorda poi che scaricare file audio e video (o comunque grandi quantità di dati) è in grado di degradare le prestazioni offerte dal servizio agli altri utenti: per tale motivo ciò può avvenire solo se necessario e, possibilmente, al di fuori dei momenti "di punta" a livello di Istituto.

Per garantire la sicurezza informatica ed il controllo del corretto utilizzo dell'accesso ad Internet l'istituto si è dotato di strumenti specifici che consentono:

- La protezione da accessi non autorizzati provenienti da Internet
- Controlli antivirus centralizzati
- configurazione di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (quali a titolo esemplificativo e non esaustivo: l'accesso ai siti inseriti in black list individuati dall'Istituto, il download di file o software aventi particolari caratteristiche dimensionali o di tipologia di dato), anche in modo differenziato per le diverse postazioni o tipologie di accesso;
- la determinazione di informazioni sulla navigazione Internet che consentono la conservazione di informazioni relative ad utente, PC, ora di accesso, pagine accedute, etc.

Si precisa che ulteriori tracce dell'operato di ciascun utente, lasciate sui PC, sui server e sui programmi impiegati, potranno essere utilizzate per l'individuazione e la sanzione di eventuali comportamenti anomali.

La conservazione nel tempo dei dati relativi all'uso degli strumenti informatici verrà fatta per il periodo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza ovvero in adempimento di obblighi previsti dalla legge;

7. Trattamenti esclusi

L'Istituto Scolastico non effettua controlli prolungati, costanti o indiscriminati dell'uso di Internet e Posta elettronica da parte dei dipendenti.

L'Istituto Scolastico non effettua trattamenti di dati personali mediante sistemi hardware e software che mirano al controllo a distanza di lavoratori attraverso:

- lettura e registrazione sistematica dei messaggi di posta elettronica personali dei dipendenti o dei relativi dati esteriori;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- lettura e registrazione dei caratteri inseriti dai lavoratori tramite la tastiera ovvero dispositivi analoghi a quello descritto;

8. Gradualità dei controlli

1. Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il Dirigente Scolastico può adottare eventuali misure che consentano la verifica di comportamenti anomali.
2. Per quanto possibile, sarà preferito un controllo preliminare su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree. Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti d'Istituto e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
3. La presenza di successive anomalie potrà comportare controlli su base individuale.
4. La rilevazione delle anomalie e delle verifiche tecniche è a cura dell'Amministratore di Sistema che potrà anche intervenire su richiesta del Dirigente Scolastico per la verifica di situazioni anomale o sospette.
5. Responsabile dei successivi e consequenziali provvedimenti è il Dirigente Scolastico.

9. Sanzioni

1. È fatto obbligo a tutti i Lavoratori di osservare le disposizioni del presente disciplinare e qualunque altra comunicata dall'Amministrazione in materia di sicurezza e gestione delle attrezzature informatiche.
2. Il mancato rispetto o la violazione delle regole contenute nel presente Disciplinare è perseguibile con tutte le azioni civili e penali previste dalla legge, nonché con i provvedimenti disciplinari, in conformità a quanto previsto dalle disposizioni normative e contrattuali vigenti per il personale o per l'area dirigenza del comparto Regioni ed Autonomie Locali. Rimane ferma ogni ulteriore forma di responsabilità civile e penale, quali ad es.:
   - violazione della privacy e della tutela dell'immagine;
   - diffamazione;
   - accesso abusivo ad un sistema informatico e telematico;
   - violazione della legge sul copyright.
3. Il codice di comportamento ed il codice disciplinare sono consultabili nel sito internet dell'Ente

10. Disposizioni ulteriori

1. I dati personali inerenti i Lavoratori non possono essere portati a conoscenza di terzi non autorizzati. I colleghi di lavoro della persona interessata sono considerati terzi.
2. L'Amministrazione, nell'ambito di procedimenti disciplinari e/o di procedimenti penali di cui all'art. 11 del presente Disciplinare e nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza del Lavoratore, procede alla conservazione delle "registrazioni a giornale" (log file) relative all'utilizzazione di Internet e/o della Posta Elettronica e/o dei files delle telefonate e/o dei Fax e dei Fax mail, fino alla conclusione dei relativi procedimenti.

3. Il presente documento viene portato a conoscenza di tutti i Lavoratori, indicati all'art. 1 del presente Disciplinare, mediante pubblicazione nei sito internet.

11.Aggiornamento periodico

Il presente regolamento è aggiornato con cadenza almeno annuale o in caso di rinvenimento di soluzioni tecnologiche ritenute più idonee a tutelare i dati personali dei lavoratori, e portato a conoscenza di tutti i lavoratori mediante affissione all'albo dell'istituto e pubblicazione nell'intranet istituzionale.

13. Entrata in vigore del regolamento e pubblicità

Il nuovo regolamento entrerà in vigore il giorno successivo alla data di pubblicazione all'albo pretorio online di Istituto.
Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
Copia del regolamento, oltre ad essere affisso in bacheca, verrà consegnato
Individualmente a ciascun utente informatico di segreteria.

IL DIRIGENTE SCOLASTICO
(Dott. Roberto Navarra)

Firma autografa sostituita a mezzo stampa ai sensi dell'Art. 3, comma 2, del D.Lgs. 39/93.

Approvato da Consiglio d'Istituto in data 11/11/2014