

DISCIPLINARE INTERNO SULL'USO DELLA POSTA ELETTRONICA E DI INTERNET

L'istituzione scolastica indicata in intestazione del presente documento (in prosieguo denominata istituto)

- Visto il D.Lgs. 196/2003 "Codice in materia di protezione dei dati personali",
- visto il Regolamento emanato dal Ministero della Pubblica Istruzione con decreto 7 dicembre 2006 n. 305;
- visto il provvedimento del Garante del 1° marzo 2007;
- considerata la necessità di contemperare l'obbligo di adozione di misure di protezione dei dati trattati con strumenti informatici e di prevenzione dei rischi che incombono sugli stessi a seguito dell'utilizzo della posta elettronica e di internet, con l'esigenza di tutelare la dignità dei lavoratori e il diritto alla riservatezza dei loro dati personali,

PREMESSA

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet, offre grandi opportunità di sviluppo, che questa Istituzione intende valorizzare e promuovere.

Tuttavia la libertà di accesso e uso crea problemi alla sicurezza dei dati, espone la scuola ai rischi patrimoniale e penali nonché relativi all'immagine dell'Istituto stesso: per questo accesso e uso devono essere regolamentati.

Premesso che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente sono basilari in un rapporto di lavoro, quanto qui riportato viene incontro quindi alla necessità di disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei dipendenti e contiene informazioni utili per comprendere cosa può fare ogni dipendente per contribuire a garantire la sicurezza informatica di tutta l'Istituto.

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.

La DIREZIONE DIDATTICA STATALE II CIRCOLO garantisce che il trattamento dei dati personali dei dipendenti, effettuato per verificare il corretto utilizzo della posta elettronica e di Internet, si conforma ai principi di necessità, correttezza, pertinenza e non eccedenza.

Le prescrizioni riportate si aggiungono e integrano le norme già previste dai contratti di lavoro dalla normativa vigente e dal DPS.

Adotta

il presente disciplinare al fine di descrivere le caratteristiche e le regole di utilizzo della rete Internet e della posta elettronica e di informare i lavoratori sui controlli effettuati e sul trattamento eseguito sui loro dati personali, in conseguenza delle misure adottate per la protezione degli strumenti informatici.

misure di tipo organizzativo connesse a
ACCESSO E USO RETE DI ISTITUTO, INTERNET E POSTA ELETTRONICA

La DIREZIONE DIDATTICA STATALE II CIRCOLO ha provveduto ad un'attenta valutazione dell'impatto dei necessari controlli sui diritti dei lavoratori ed ha, conseguentemente, ridotto i controlli stessi al minimo indispensabile a garantire la sicurezza dei servizi di rete.

Per quanto concerne l'individuazione dell'ubicazione riservata alle postazioni di lavoro, al fine di ridurre il rischio di impieghi abusivi, si specifica che ogni unità di personale ATA che svolge le proprie funzioni specificamente su postazione informatica riceve indicazione della postazione di lavoro a lui assegnata al momento della presa di servizio, ovvero in caso di cambiamento della propria posizione.

L'accesso alle postazioni è protetto tramite sistema di autenticazione che richiede l'immissione di un apposito codice utente e della relativa password.

Le proprie credenziali di accesso devono essere conservate segrete con cura e, ovviamente, non devono essere assolutamente comunicate ad altri: di qualsiasi azione o attività svolta utilizzando il codice identificativo e/o la password assegnata è responsabile l'utente assegnatario del codice.

Si raccomanda ad ogni dipendente di:

- non cedere o lasciare incustodita, una volta superata la fase di autenticazione, la propria postazione;
- conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata a processi di autenticazione personale;
- non utilizzare credenziali (user-id e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;
- mantenere la corretta configurazione del proprio computer non alterando le componenti hardware e software predisposte allo scopo né installando ulteriori software non autorizzati;
- non connettere in rete stazioni di lavoro se non dietro esplicita autorizzazione dell'amministratore di sistema (o utilizzare comunque la rete d'istituto per fini non espressamente autorizzati);
- ricordarsi di spegnere il computer terminato il turno di lavoro;
- è consentito salvare su server e computer dell'Istituto solo dati di carattere lavorativo (in quanto ai dati salvati su computer dell'Istituto potranno accedere altri dipendenti, in base a competenze e funzioni);
- l'eventuale cancellazione di file temporanei, percorsi di navigazione (ultimi siti visitati), ecc... è a cura di chi li ha generati.

Si ricorda infine che i computer dell'Istituto sono affidati ai dipendenti come strumento di lavoro.

Ognuno è responsabile dell'utilizzo delle dotazioni informatiche, fisse o mobili, ricevute in assegnazione.

Vanno quindi evitati utilizzi non inerenti all'attività lavorativa (che possono inoltre contribuire ad innescare disservizi, costi di manutenzione e minacce alla sicurezza).

misure di tipo tecnologico connesse a
UTILIZZO DELLA POSTA ELETTRONICA

Il MIUR mette a disposizione di ogni dipendente una casella personale sul dominio istruzione.it, (ad es., del tipo nome.cognome@istruzione.it).

Per tale casella il MIUR ha pubblicato le “POLITICHE DI UTILIZZO DEL SERVIZIO DI POSTA ELETTRONICA PER GLI UTENTI STANDARD DEL DOMINIO istruzione.it” (reperibile sul sito istituzionale del Ministero): tutto il personale è tenuto a conoscere e rispettare quanto indicato in tale documento.

Ai fini di questo “disciplinare interno” è utile ricordare, per le caselle personali sul dominio istruzione.it, 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.

Tutta la comunicazione di interesse amministrativo e di lavoro deve pervenire alla scuola sugli indirizzi non personali, si ottiene così una ottimale separazione tra la sfera personale e quella lavorativa.

Per tale motivo non è necessaria alcuna politica che consenta a questa Istituzione di accedere alle caselle personali nome.cognome@istruzione.it dei dipendenti in caso di assenza né di far disporre meccanismi di risposta automatica.

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: su dominio dell'Istituto TOEE09600X@istruzione.it, circolo2chieri@tiscali.it, caselle PEC istituzionali (segreteria@pec.circolo2chieri.it, TOEE09600X@pec.istruzione.it).

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).

Gestendo 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 (quali, ad es. circolo2chieri@tiscali.it, ecc.), 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 (ancor più critiche in ambito lavorativo), si aggiungono le seguenti disposizioni:

- Nel caso di messaggi provenienti da mittenti sconosciuti e che contengono allegati sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd,...), questi ultimi non devono essere aperti: eventualmente, 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 (*.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.

Le modalità di gestione delle diverse caselle sono fissate in base alle funzioni. E' comunque utile rimarcare che la gestione delle caselle di Posta Certificata deve essere effettuata in stretto contatto con la dirigenza (D.S. o D.S.G.A.) e che:

- di ogni ricezione di messaggi sulla casella TOEE09600X@pec.istruzione.it, segreteria@pec.istruzione.it, deve essere tempestivamente informato il Dirigente Scolastico (o il suo sostituto);
- ogni invio tramite la casella TOEE09600X@pec.istruzione.it, segreteria@pec.istruzione.it, deve essere esplicitamente disposto dal Dirigente Scolastico (o dal suo sostituto).

misure di tipo tecnologico connesse a
NAVIGAZIONE IN INTERNET

La DIREZIONE DIDATTICA STATALE II CIRCOLO 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".

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 o similari (salvo specifiche attività espressamente autorizzate per le finalità istituzionali).
- 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..)
- 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.

MONITORAGGIO, CONTROLLI E SANZIONI

La DIREZIONE DIDATTICA STATALE II CIRCOLO può avvalersi di sistemi di controllo del corretto utilizzo degli strumenti di lavoro; l'eventuale regolazione e monitoraggio del traffico di rete avverrà secondo le seguenti modalità e principi:

- configurazione di sistemi o utilizzo 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;
- trattamento di dati in forma aggregata;
- conservazione nel tempo dei dati per il periodo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza ovvero in adempimento di obblighi previsti dalla legge;

Trattamenti esclusi :

La DIREZIONE DIDATTICA STATALE II CIRCOLO non effettua controlli prolungati, costanti o indiscriminati dell'uso di Internet e Posta elettronica da parte dei dipendenti.

La DIREZIONE DIDATTICA STATALE II CIRCOLO 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;
- analisi occulta dei dispositivi per l'accesso ad Internet o l'uso della posta elettronica messi a disposizione dei dipendenti.

Graduazione dei controlli:

- 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.
- 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 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.
- La presenza di successive anomalie potrà comportare controlli su base individuale.

Il personale deve inoltre attenersi alle disposizioni in materia di sicurezza e a quanto disposto con il DPS.

La violazione delle disposizioni riportate nel presente disciplinare può comportare l'applicazione delle sanzioni disciplinari previste dalle vigenti norme e Contratti di Lavoro.

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.

VALIDITA', AGGIORNAMENTO E REVISIONE

Il seguente Disciplinare interno entra in vigore a partire dal 1° giorno del mese successivo a quello di approvazione.

Tutti i dipendenti possono proporre, quando ritenuto necessario, integrazioni al presente regolamento tramite comunicazione al Consiglio di Circolo.

In occasione dell'aggiornamento del DPS, il Dirigente Scolastico valuterà poi l'eventuale necessità di proporre modifiche al presente disciplinare, che conserva comunque validità permanente fino a successiva revisione.

CHIERI, 29/03/2011

Il Dirigente scolastico
GALLO MARIO