Disciplinare interno

- **per l’utilizzo della posta elettronica ed Internet nel rapporto di lavoro e nel rapporto formativo**
- **per l’utilizzo delle apparecchiature informatiche**
- **per l’amministrazione delle risorse informatiche**

Sommario

Art. 1 Oggetto e ambito di applicazione

Il presente regolamento disciplina l'utilizzo nel rapporto di lavoro e formativo della posta elettronica e rete Internet secondo quanto previsto dalle linee guida del Garante del 01/03/2007 in gazzetta Ufficiale n. 58 del 10/3/2007 nonché l'utilizzo delle apparecchiature e infrastrutture informatiche della scuola e del suo patrimonio informativo digitale.

Il presente regolamento si applica a tutti gli utenti Interni ed Esterni che sono autorizzati ad accedere alle apparecchiature e infrastrutture informatiche della scuola e al suo patrimonio informativo digitale. Per utenti Interni si intendono tutti gli Assistenti Amministrativi, il Direttore SGA e il Dirigente Scolastico, i Collaboratori scolastici, i Docenti e gli Alunni. Per utenti Esterni si intendono le ditte fornitrici di software che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza e la ditta incaricata della manutenzione hardware e software delle risorse infrastrutturali.

Art. 2 - Principi generali – Diritti e Responsabilità

L'Istituto promuove l'utilizzo della Rete Informatica e Telematica, di Internet e della Posta Elettronica quali strumenti utili a perseguire le proprie finalità istituzionali.

Ogni utente è responsabile civilmente e penalmente del corretto uso delle Risorse informatiche, in particolare di quelle che ha ricevuto in consegna, dei Servizi/programmi ai quali ha accesso e dei propri dati.

I docenti vigilano inoltre sull'uso che gli studenti loro affidati fanno delle apparecchiature e infrastrutture informatiche della scuola e del suo patrimonio informativo digitale.

Il presente regolamento considera i divieti posti dallo Statuto dei lavoratori sul controllo a distanza (artt.113, 114 e 184, comma 3, del Codice; artt. 4 e 8 legge 20 maggio 1970, n.300), rispettando durante i trattamenti i principi di necessità (art. 3 del Codice), correttezza (art. 11, comma 1, lett. a), pertinenza e non eccedenza (art. 11, comma 1, lett. d).

Per motivi di sicurezza e protezione dei dati, ogni attività compiuta nella Rete Informatica degli Uffici è sottoposta a registrazione in appositi file e riconducibili

ad un account di rete. Detti file possono essere soggetti a trattamento solo per fini istituzionali, per attività di monitoraggio e controllo e possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente. La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal D.Lgs. n. 196/2003.

A tutela del dipendente, qualora l'Istituto decidesse di perseguire, per fini legati alla sicurezza dell'intero sistema informativo, il controllo della posta e della navigazione in internet, prima di iniziare il trattamento comunicherà gli strumenti e i modi di trattamento effettuati. Tale compito sarà effettuato/demandato ad una società esterna a garanzia e tutela delle informazioni di carattere personale dei lavoratori subordinati.

L'Amministratore di Sistema cura l'attuazione del presente regolamento, in particolare per la registrazione delle attività compiute nella rete della segreteria dai vari utenti egli si avvale degli eventviewer di windows sia a livello di singola macchina che di server (controllo eventi accesso account e controllo eventi di accesso).

Il presente regolamento è affisso all'Albo d'Istituto; esso è disponibile per la consultazione sulla rete telematica della Segreteria e sul sito web istituzionale.

Art. 3 - Utilizzo dei PERSONAL COMPUTER.

Il Personal Computer affidato al dipendente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza e pertanto è vietato.

In particolare per la Rete degli Uffici:

a) L'accesso all'elaboratore deve essere protetto da password personale e non cedibile che deve essere custodita da ogni utente con la massima diligenza e non divulgata. La password deve essere attivata per l'accesso alla rete, per lo screensaver e per il software applicativo.

b) L'Amministratore di Sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha la facoltà di accedere in qualunque momento, con il proprio account, al personal computer di ciascuno;

c) Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. Lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. Deve essere attivato su tutti i Personal Computer lo screen saver e la relativa password;
d) L'accesso ai dati presenti nel personal computer potrà avvenire quando si rende indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato;
e) È vietato installare autonomamente programmi informatici salvo autorizzazione esplicita dell'Amministratore di Sistema, in quanto sussiste il grave pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la struttura a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 sulla tutela giuridica del software e L.248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
f) È vietato modificare le caratteristiche impostate sul proprio PC, salvo con autorizzazione esplicita dell'Amministratore di Sistema;
g) È vietato inserire password locali alle risorse informatiche assegnate (come ad esempio password che non rendano accessibile il computer agli amministratori di rete), se non espressamente autorizzati e dovutamente comunicate all'Amministratore di Sistema;
h) È vietata l'installazione sul proprio PC di dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, pendrive, dischi esterni, i-pod, telefoni, ecc.), se non con l'autorizzazione espressa dell'Amministratore di Sistema. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti.

Per le infrastrutture ad uso didattico e dei docenti valgono le stesse regole previste per la Rete degli Uffici con le seguenti precisazioni:

i) Il ruolo di gestore delle password e le autorizzazioni alle installazioni di programmi ed in generale tutti i compiti affidati per la rete degli Uffici all'Amministratore di sistema, vengono svolti dal responsabile del laboratorio, se di laboratorio si tratta, o dal sub-consegnatario del bene(coordinatore di plesso)

j) Le disposizioni del presente disciplinare integrano quelle del regolamento d'uso del laboratorio informatico.

Art. 4 - Utilizzo della RETE INFORMATICA degli Uffici e dei Laboratori.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali sulle quali vengono svolte regolari attività di controllo, amministrazione e backup e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato in queste unità, nemmeno per brevi periodi.

Si parte quindi dal presupposto che i files relativi alla produttività individuale vengono salvati sul server e i limiti di accesso sono regolarizzati da apposite policies di sicurezza che suddividono gli accessi tra gruppi e utenti.

L'amministratore di Sistema per gli Uffici e il responsabile di laboratorio per i laboratori possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza o in violazione del presente regolamento sia sui PC degli incaricati sia sulle unità di rete.

Le password d'ingresso alla rete ed ai programmi sono segrete e non vanno comunicate a terzi.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

E' importante togliere tutte le condivisioni dei dischi o di altri supporti configurate nel Personal Computer se non strettamente necessarie (e per breve tempo) allo scambio dei files con altri colleghi. Esse sono infatti un ottimo "aiuto" per i software che cercano di "minare" la sicurezza dell'intero sistema.

E’ attiva sul server un’area condivisa per lo scambio dei dati tra i vari utenti.
Nell’utilizzo della rete informatica è fatto divieto di:
a) Utilizzare la Rete in modo difforme da quanto previsto dal presente regolamento;
b) Conseguire l’accesso non autorizzato a risorse di rete interne ed esterne alla Rete dell’Istituto;
c) Agire deliberatamente con attività che influenzino negativamente la regolare operatività della Rete e ne restringano l’utilizzabilità e le prestazioni per altri utenti;
d) Effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);
e) Installare componenti hardware non compatibili con l’attività istituzionale;
f) Rimuovere, danneggiare o asportare componenti hardware;
g) Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti;
h) Utilizzare software visualizzatori di pacchetti TCP/IP (sniffer), software di intercettazione di tastiera (keygrabber o keylogger), software di decodifica password (cracker) e più in generale software rivolti alla violazione della sicurezza del sistema e della privacy;
i) Usare l’anonimato o servirsi di risorse che consentano di restare anonimi;

Art. 5 - Utilizzo di INTERNET

l Personal Computer, qualora abilitati alla navigazione in Internet, costituiscono uno strumento necessario allo svolgimento della propria attività lavorativa.
Nell’uso di Internet e della Posta Elettronica non sono consentite le seguenti attività:
a) L’uso di Internet per motivi personali;
b) L’accesso a siti inappropriati (esempio siti pornografici, di intrattenimento, ecc.);
c) Lo scaricamento (download) di software e di file non necessari all’attività istituzionale;

d) Utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Winmx, e-Donkey, ecc.);
e) Accedere a flussi in streaming audio/video da Internet per scopi non istituzionali (ad esempio ascoltare la radio o guardare video o filmati utilizzando le risorse Internet);
f) Un uso che possa in qualche modo recare qualsiasi danno all'Istituto o a terzi;
Presso il laboratorio multimediale è attivo un firewall con filtro sui contenuti Internet tenuto costantemente aggiornato.
La vigilanza e la responsabilità per quanto attiene al traffico internet effettuato dagli studenti è a carico dei docenti a cui sono affidati. In sintesi gli studenti non devono accedere a internet, in particolare dove non è attivo alcun filtro contenuti, senza sorveglianza/supervisione da parte di un docente.

Art. 6 - Utilizzo della POSTA ELETTRONICA

La casella di posta, assegnata dal Ministero, è uno strumento di lavoro.
Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica della struttura per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
La documentazione elettronica che viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto, non può essere comunicata all'esterno senza preventiva autorizzazione del Responsabile del trattamento.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

È obbligatorio controllare i file Attachments di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web, HTTP o FTP non conosciuti) e accertarsi dell'identità del mittente.
In particolare nell'uso della Posta Elettronica non sono consentite le seguenti attività:
a) La trasmissione a mezzo di posta elettronica di dati sensibili, confidenziali e personali di alcun genere, salvo i casi espressamente previsti dalla normativa vigente in materia di protezione dei dati personali (D.lgs. 196 del 30/6/2003);
b) L'apertura di allegati ai messaggi di posta elettronica senza il previo accertamento dell'identità del mittente;
c) Inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici;
d) Inoltrare "catene" di posta elettronica.
Quanto detto su vigilanza e responsabilità per quanto attiene al traffico internet effettuato dagli studenti vale anche per la posta elettronica. Anche l'uso da parte degli studenti della posta elettronica deve osservare per quanto possibile il presente regolamento, soprattutto il non utilizzo di posta personale né attraverso l'uso di un webmail né utilizzando un client di posta.

Art. 7 - Utilizzo delle PASSWORD nella Rete della Segreteria

Le password di ingresso alla rete di segreteria, di accesso ai programmi e dello screen saver, sono previste ed attribuite dall'Amministratore di Sistema ad ogni Utente del Gruppo di lavoro.
E' necessario procedere alla modifica della password a cura di ogni utente del gruppo di lavoro, al primo utilizzo e, successivamente, almeno ogni tre mesi (come previsto dal punto 5 del disciplinare tecnico allegato al Codice della privacy, D.lgs. n.196/2003), su ogni PC sul quale ha un account con contestuale comunicazione all'Amministratore di Sistema, che lo inviterà a modificare anche sul Server, in maniera guidata, la propria password.
L'Amministratore di Sistema sovraintende alla variazione della password nei tempi previsti dalla norma e dal presente regolamento sollecitando i vari Utenti eventualmente in ritardo.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato (punto 5 del disciplinare tecnico).
La password deve essere immediatamente sostituita, dandone comunicazione scritta all'Incaricato della custodia delle Password, nel caso si sospetti che la stessa abbia perso la segretezza. Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia, per iscritto, all'Amministratore di Sistema dell'Istituto.

Art. 8 - Utilizzo dei SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato (punto 22 del disciplinare tecnico).
I supporti magnetici contenenti dati sensibili e giudiziari devono essere custoditi in archivi chiusi a chiave.
Tutti i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) obsoleti devono essere consegnati all'Amministratore di Sistema per l'opportuna distruzione.
Ogni qualvolta si procederà alla dismissione di un Personal Computer l'Amministratore di Sistema provvederà alla distruzione delle unità di memoria interne alla macchina stessa (hard-disk, memorie allo stato solido).

Art. 9 - Utilizzo di PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

L’utilizzo di un PC portatili all’esterno dell’Istituto per convegni, corsi aggiornamento, ecc. deve essere richiesto/comunicato preliminarmente al Direttore SGA, consegnatario dei beni mobili dell’istituto, o al sub-consegnatario del bene.

Art. 10 - Utilizzo delle stampanti e dei materiali di consumo

L’utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) è riservato esclusivamente ai compiti di natura strettamente istituzionale.

Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi.

È cura dell’utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

Art. 11 - Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di incaricato del trattamento dei dati ai sensi del disciplinare tecnico allegato al D.lgs. n. 196/2003.

Art. 12 - Amministrazione di sistema

L’Amministratore di sistema è il soggetto a cui il datore di lavoro conferisce il compito di sovrintendere alle risorse informatiche dell’Istituto e a cui sono consentite le seguenti attività:

- sovrintendere al funzionamento della rete e monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza informatica;
- effettuare interventi di manutenzione hardware e software sui sistemi operativi e applicativi;
- aggiornare con frequenza almeno annuale(semestrale se si trattano dati sensibili e giudiziari)i programmi volti a prevenire la vulnerabilità degli

strumenti elettronici e a correggere i difetti (firewall, filtri per la posta elettronica, antivirus,ecc.);

- predisporre ed implementare le ulteriori misure minime di sicurezza imposte dal disciplinare per il trattamento informatico dei dati sensibili e giudiziari e per la conseguente tutela degli strumenti elettronici;
- predisporre e rendere funzionanti le copie di sicurezza dei dati e delle applicazioni e impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale;
- predisporre un piano dei controlli periodici da eseguirsi con cadenza almeno annuale , dell'efficacia delle misure di sicurezza adottate dell'Istituto;
- verificare che l'Istituto abbia adottato le misure minime di sicurezza per il trattamento dei dati personali.

Apparecchiature e infrastrutture informatiche ad uso didattico

I compiti assegnati all'Amministratore di Sistema per la rete degli Uffici possono essere svolte dai sub-consegnatari delle apparecchiature o dai responsabili di laboratorio.

Nell'esercizio di tali compiti possono avvalersi della consulenza dell'Amministratore di Sistema e/o, tramite di esso della Ditta che si occupa della manutenzione hardware e software del patrimonio informatico dell'Istituto.

Art. 13 - Non osservanza del regolamento

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente, comporta l'immediata revoca delle autorizzazioni ad accedere alla Rete Informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni più gravi previste dalle norme vigenti.

Se i lavoratori perseverassero nell'uso ed abuso degli strumenti elettronici a loro disposizione, il datore è autorizzato a procedere per step, con controlli prima sul

reparto, poi sull’ufficio ed, infine, sul gruppo di lavoro; solo a questo punto, ripetendosi l’anomalia, sarà lecito il controllo su base individuale.

Art. 14 - Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dall’Amministratore di Sistema e dal Dirigente Scolastico. Il presente Regolamento è soggetto a revisione con frequenza annuale entro il 31 marzo di ogni anno.