ISTITUTO COMPRENSIVO "G. TONIOLO" PISA
Via Niosi n°4 - 56125 PISA – tel. 050/24528 – fax 050/504163

Disciplinare interno per l'utilizzo delle strumentazioni informatiche, della rete internet e della posta elettronica da parte del personale e degli studenti

Premesso che compete al datore di lavoro:
- assicurare la funzionalità delle strumentazioni informatiche in dotazione all'istituto ;
- adottare idonee misure di sicurezza per garantire la disponibilità e l'integrità dei sistemi informativi e dei dati, nonché per prevenire utilizzi indebiti;
- adottare limiti e cautele per evitare la registrazione e diffusione di fotografie e i filmati in tempo reale anche utilizzando i terminali di nuova generazione applicati alla telefonia mobile;
- indicare in modo particolareggiato quali siano gli strumenti messi a disposizione le modalità di utilizzo nell'organizzazione dell'attività lavorativa e/o di studio degli strumenti messi a disposizione dei dipendenti e degli studenti ritenute corrette;
- precisare in che misura e con quali modalità vengano effettuati i controlli;
- tutelare i lavoratori interessati nel trattamento di dati per finalità di gestione del rapporto in ambito pubblico, adottando quelle misure che garantiscono un elevato standard di sicurezza e garanzia;
- tener conto della normativa in tema di informazione, concertazione e consultazione delle organizzazioni sindacali,

sono stabilite le prescrizioni del presente disciplinare di seguito riportate che si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati del trattamento dati in attuazione del D.Lgs. 30 giugno 2003 n. 196 e del Disciplinare tecnico (Allegato B al citato decreto legislativo allegato) e a cui devono attenersi tutti gli utilizzatori (personale e studenti, d'ora in poi definiti *utenti)* delle strumentazioni informatiche, della rete internet e della posta elettronica.

Finalità
Il presente regolamento disciplina le modalità di accesso e di uso della Rete Informatica, telematica e dei servizi che, tramite la Rete stessa, è possibile ricevere o offrire all'interno e all'esterno dell'Istituto per dare il supporto informativo, documentario, alla ricerca, alla didattica, all'aggiornamento e alle attività collaborative tra scuole ed enti, nonché per tutti gli adempimenti amministrativi di legge.

Ambito di applicazione
La Rete dell'Istituto..... è costituita dall'insieme delle Risorse informatiche, cioè
- dalle componenti hardware/software e dagli apparati elettronici collegati alla Rete Informatica dell'Istituto
- dall'insieme delle banche dati in formato digitale ed in generale di tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.

Il presente regolamento si applica, senza distinzione di ruolo e/o livello, a tutti gli *utenti* interni (personale amministrativo, docenti e collaboratori scolastici) autorizzati ad accedere alla Rete della scuola nell'ambito della propria attività lavorativa ordinaria e straordinaria e agli studenti nei limiti loro assegnati a scopi didattici ed educativi. Analogamente il presente regolamento si applica alle ditte che effettuano attività di manutenzione, agli eventuali altri soggetti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle convenzioni stesse nel rispetto del presente disciplinare tecnico e a tutti i collaboratori dell'Istituto a prescindere dal rapporto contrattuale con gli stessi intrattenuto (es. soggetto in stage, ecc.).

Principi generali
L'istitutoComprensivo Toniolo di Pisa prevede l'utilizzo delle strumentazioni informatiche, della rete Internet e della posta elettronica da parte degli *utenti* quali strumenti utili a perseguire le proprie finalità istituzionali e prevede che lo stesso si conformi ai seguenti principi:
1. *principio di necessità:* i sistemi informativi e i programmi informatici vengono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
2. *principio di correttezza:* le caratteristiche essenziali dei trattamenti sono rese note ai lavoratori;
3. *principio di pertinenza e non eccedenza*: i trattamenti sono effettuati per finalità determinante, esplicite e legittime e i dati sono trattati nella misura meno invasiva possibile.

Valutazione del rischio
La rete informatica di istituto, l'accesso alla rete internet e alla posta elettronica, il PC affidato al dipendente sono strumenti di lavoro; su di essi vengono effettuate regolari attività di controllo, amministrazione e backup ed essi non possono in alcun modo essere utilizzati per scopi diversi perché ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
In relazione all'utilizzo non corretto di detti strumenti si individuano I seguenti possibili rischi e conseguenti effetti:

Attività	*Rischio*	*Motivazione*	*Possibile effetto*
Manutenzione di periferiche hardware interne (scheda video, memoria, ecc.)	Alto	Possono essere danneggiati componenti interni e il PC	Danneggiamento dei PC
Manutenzione di periferiche hardware esterne (tastiere, mouse, ecc.)	Basso		
Download non controllato o non programmato di aggiornamenti relativi ad applicazioni installate dal responsabile di rete	Alto	Possono essere scaricate applicazioni non verificate con il pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore.	Danneggiamento del software del PC o della rete informatica interna.
Download controllato o programmato di aggiornamenti relativo ad applicazioni installate dal responsabile di rete	Basso		
Download di dati non inerenti alle attività lavorative (musica, giochi, ecc.)	Alto	Possono essere scaricate applicazioni non verificate con il pericolo di portare Virus informatici o di alterare la stabilità delle applicazioni dell'elaboratore.	Danneggiamento del software del PC o della rete informatica. Gravi responsabilità civili e penali per l'Istituto in caso di violazione della normativa a tutela dei diritti d'autore.
Installazione di applicazioni senza l'autorizzazione del responsabile della rete	Alto	Possono essere installate applicazioni non compatibili	Danneggiamento del software del PC o della rete informatica interna.
Accesso alla rete effettuato da PC di proprietà dell'utente	Alto	Accessi non autorizzati alla rete	Furto di dati
Download delle e-mail	Medio/ Alto		
Apertura di allegati di posta elettronica di incerta provenienza	Alto	Contenere Malware/Spyware	Danneggiamento del software del PC o della rete informatica interna Divulgazione di password e dati riservati
Elaboratore connesso alla rete lasciato incustodito o divulgazione di password	Alto	Possibile utilizzo da parte di terzi.	Uso indebito di dati riservati, danneggiamento della rete informatica interna.
Utilizzo di supporti removibili esterni non autorizzati	Alto	Possono essere trasferite applicazioni dannose per il PC nella rete informatica	Danneggiamento dei PC o della rete informatica interna Furto di dati
Mancata distruzione o perdita accidentale di supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) contenenti dati sensibili e giudiziari.	Alto	Recupero di dati memorizzati anche dopo la loro cancellazione.	Uso indebito di dati riservati.

2. MISURE DI TIPO ORGANIZZATIVO

Assegnazione delle postazioni di lavoro

Per ridurre il rischio di impieghi abusivi o dannosi, il datore di lavoro provvede a :

- individuare preventivamente le postazioni di lavoro e assegnarle personalmente a ciascun dipendente;
- individuare preventivamente gli utenti a cui è accordato l'utilizzo della posta elettronica e l'accesso a Internet.

La strumentazione dell'Istituto non è di esclusivo dominio del dipendente, ma rientra tra i beni a cui determinati soggetti possono comunque sempre accedere. L'eventuale accesso del datore di lavoro , qualora necessiti di informazioni contenute nei documenti residenti sul PC assegnato al dipendente, è legittimo.

Nomina dell'Amministratore di sistema

Il datore di lavoro conferisce agli Amministratore di Sistema il compito di sovrintendere alle Risorse Informatiche dell'Istituto assegnandogli in maniera esclusiva le seguenti attività:

a. gestione dell'hardware e del software (installazione, aggiornamento, rimozione) di tutte le strutture tecniche informatiche dell'Istituto, siano esse collegate in rete o meno;
b. configurazione dei servizi di accesso alla rete interna, ad Internet e a quelli di posta elettronica con creazione, attivazione e disattivazione dei relativi account.
c. creazione di un'area condivisa sul server per lo scambio dei dati tra i vari utenti, evitando condivisioni dei dischi o di altri supporti configurati nel Personal Computer che non siano strettamente necessarie perché sono un ottimo "aiuto" per i software che cercano di "minare" la sicurezza dell'intero sistema;
d. controllo del corretto utilizzo delle risorse di rete, dei computer e degli applicativi, durante le normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
e. rimozione, sia sui PC degli incaricati sia sulle unità di rete, di ogni file o applicazione che può essere pericoloso per la Sicurezza o costituisce violazione del presente regolamento;
f. distruzione delle unità di memoria interne alla macchina (hard-disk, memorie allo stato solido) ogni qualvolta si procederà alla dismissione di un PC e dei supporti removibili consegnati a tale scopo dagli utenti;
g. utilizzo delle credenziali di amministrazione del sistema per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di indispensabile ed indifferibile necessità di intervento per prolungata assenza, irrintracciabilità o impedimento dello stesso, ma solo per il tempo strettamente necessario al compimento di attività indifferibili e solo su richiesta del Responsabile del trattamento.

L'Amministratore di Sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, e dopo aver richiesto l'autorizzazione all'utente interessato, al personal computer di ciascun utente.

Utilizzo delle password

UTILIZZAZIONE DI UN SISTEMA DI AUTORIZZAZIONE

Per l'accesso alla strumentazione informatica di Istituto ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione previste ed attribuite dall'Incaricato della custodia delle Password. Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal custode delle password e consistono in un codice per l'identificazione dell'utente *(user id),* associato ad una parola chiave (*password)* riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non può essere divulgata. Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

- la password di accesso al computer impedisce l'utilizzo improprio della postazione, quando per un motivo o per l'altro l'incaricato non si trova in ufficio;

- la password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'ufficio;
- la password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato;
- la password del salvaschermo, infine, impedisce che una assenza momentanea permetta a una persona non autorizzata di visualizzare il lavoro dell'incaricato.

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).

PROCEDURE DI GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE

a. È necessario procedere alla modifica della parola chiave, a cura dell'incaricato, al primo utilizzo. Se l'utente non provvede autonomamente a variare la password entro i termini massimi, viene automaticamente disabilitato. Provvederà l'Amministratore di Sistema a riabilitare l'utente ed assegnargli una password provvisoria che l'utente dovrà cambiare al primo accesso.
b. Per scegliere la nuova parola chiave si devono seguire le seguenti istruzioni:
- usare una parola chiave di almeno otto caratteri;
- usare una combinazione di caratteri alfabetici e numerici: meglio ancora è inserire almeno un segno di interpunzione o un carattere speciale;
- non usare mai il proprio nome o cognome, né quello di congiunti (coniuge, figli, genitori), di animali domestici o date di nascita, numeri di telefono etc.. Le migliori password sono quelle facili da ricordare ma, allo stesso tempo, difficili da indovinare, come quelle che si possono ottenere comprimendo frasi lunghe.

c. La password deve essere cambiata a intervalli regolari a cura dell'incaricato del trattamento d'intesa con il Custode delle password. (*L'intervallo raccomandato per il cambio può andare da tre mesi -nel caso di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici- fino a due anni).*
d. La variazione delle password deve essere comunicata al custode delle password, a cui dovrà essere consegnata in busta chiusa con data e firma dell'incaricato apposte sul lembo di chiusura, perché ne curi la conservazione.
e. È necessario curare la conservazione della propria parola chiave e bisogna evitare di comunicarla ad altri, di trascriverla su supporti (agenda, post-it, ecc.) che siano accessibili ad altri o di consentire che qualcuno sbirci quello che si sta battendo sulla tastiera quando viene immessa la password.
f. 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.
g. Nel caso si sospetti che la password abbia perso la segretezza essa deve essere immediatamente sostituita, dandone comunicazione scritta all'Incaricato della custodia delle Password.

Utilizzo di internet

La navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. L'accesso a Internet è regolato da filtri predefiniti dall'amministratore di sistema su autorizzazione dell'amministrazione, con esclusione dei siti istituzionali.
Il titolare del trattamento provvede alla individuazione delle categorie di siti considerati correlati o non correlati con la prestazione lavorativa

Utilizzo della posta elettronica

L'istituto mette a disposizione dei lavoratori indirizzi di posta elettronica. Questi sono individuali.

3. MISURE DI TIPO TECNOLOGICO

Utilizzo della rete informatica
La rete informatica permette di salvare sul server i files relativi alla produttività individuale. Le aree di condivisione in rete sono soggette a regolari attività di controllo, amministrazione e backup.
L'accesso è regolato da apposite policies di sicurezza che suddividono gli accessi tra gruppi e utenti.
Periodicamente (almeno ogni sei mesi) si provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili.

Utilizzo di internet
L'amministratore di sistema provvede alla configurazione di sistemi e all'utilizzo di filtri che prevengono determinate operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software).

Utilizzo della posta elettronica
Sono previste apposite funzionalità di sistema che consentono:
- di inviare automaticamente in caso di assenze programmate, messaggi di risposta che contengano le coordinate di un altro soggetto o altri utili modalità di contatto del servizio presso il quale opera il lavoratore assente;
- al lavoratore, in caso di assenze improvvise o prolungate e per improrogabili necessità legate all'attività lavorativa, di delegare un collega (fiduciario) a verificare il contenuto di messaggi e a inoltrare al responsabile del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.

DIRITTI E RESPONSABILITÀ DEI DIPENDENTI

Per assicurare la tutela dei diritti, delle libertà fondamentali e della dignità dei lavoratori, garantendo che sia assicurata una ragionevole protezione della loro sfera di riservatezza nelle relazioni personali professionali, il trattamento dei dati mediante l'uso di tecnologie telematiche è conformato al rispetto dei diritti delle libertà fondamentali nonché della dignità dell'interessato, dei divieti posti dallo Statuto dei lavoratori sul controllo a distanza e dei principi di necessità, correttezza e finalità determinate, esplicite e legittime.
Ogni utente è responsabile, sia sotto il profilo civile che penale, del corretto uso delle Risorse informatiche, dei Servizi e dei programmi ai quali ha accesso e dei dati che tratta.
Spetta ai docenti vigilare affinché gli studenti loro affidati rispettino il presente regolamento (per le parti che riguardano l'attività didattica).

DOVERI DI COMPORTAMENTO DEI DIPENDENTI

Le strumentazioni informatiche, la rete Internet e la posta elettronica devono essere utilizzati dal personale e dagli studenti unicamente come strumenti di lavoro e studio. Ogni loro utilizzo non inerente all'attività lavorativa e di studio è vietato in quanto può comportare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
In particolare non può essere dislocato nelle aree di condivisione della rete alcun file che non sia legato all'attività lavorativa, nemmeno per brevi periodi.
Agli utenti è assolutamente vietata la memorizzazione di documenti informatici di natura oltraggiosa o discriminatoria per sesso lingua religione, razza, origine etnica, condizioni di salute, opinioni appartenenza sindacale politica
Non è consentito scaricare, scambiare o utilizzare materiale coperto dal diritto d'autore.
Non è consentito duplicare e/o utilizzare materiale acquisito in modo illegale anche per le attività didattiche (in particolare è vietato installare software, visualizzare o diffondere file audio e video

senza licenza d’uso, proiettare dvd, cd, vhs contenenti materiale multimediale acquisito senza regolare licenza, duplicare testi oltre quanto consentito dalla normativa vigente).

Utilizzo dei personal computer

Gli utenti utilizzano per il proprio lavoro soltanto computer di proprietà dell'istituto, salvo espresse autorizzazioni contrarie dell'Amministratore di sistema/rete, e sono tenuti a:

a. attivare sul PC lo screen saver e la relativa password;
b. conservare la password nella massima riservatezza e con la massima diligenza;
c. non inserire password locali che non rendano accessibile il computer agli amministratori di rete se non esplicitamente autorizzato dall'Amministratore di Sistema;
d. non utilizzare criptosistemi o qualsiasi altro programma di sicurezza crittografia non previste esplicitamente dal servizio informatico dell'istituto;
f. non modificare la configurazione hardware e software del proprio PC, se non esplicitamente autorizzati dall'Amministratore di Sistema;
g. non rimuovere, danneggiare o asportare componenti hardware;
h. non installare sul proprio PC dispositivi hardware personali (modem, schede audio, masterizzatori, pen- drive, dischi esterni, i-pod, telefoni, ecc.), salvo specifica autorizzazione in tal senso da parte del responsabile;
i. non installare autonomamente programmi informatici, se non esplicitamente autorizzati dall'Amministratore di Sistema;
j. non utilizzare programmi non autorizzati, con particolare riferimento ai videogiochi, che sono spesso utilizzati per veicolare virus;
j. mantenere sempre aggiornati e attivi sulla propria postazione di lavoro i software antivirus con riferimento all'ultima versione disponibile;
k. nel caso il software antivirus rilevi la presenza di un virus, sospendere immediatamente ogni elaborazione in corso senza spegnere il computer e segnalare prontamente l'accaduto al personale incaricato dell'assistenza tecnica;
i. prestare la massima attenzione ai supporti di origine esterna (es. Pen drive), verificando preventivamente tramite il programma di antivirus ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l'Amministratore di Sistema nel caso in cui vengano rilevati virus o eventuali malfunzionamenti;
m. non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
n. non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso a Internet e ai servizi di posta elettronica;
o. spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.

Utilizzo della rete informatica

Gli utenti della rete informatica sono tenuti a utilizzare la rete in modo conforme a quanto stabilito dal presente Regolamento e quindi:

a. mantenere segrete e non comunicare a terzi, inclusi gli amministratori di sistema, le password d'ingresso alla rete ed ai programmi e non permettere ad alcuno di utilizzare il proprio accesso;
b. provvedere periodicamente (almeno ogni sei mesi) alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili onde evitare un'archiviazione ridondante;
c. verificare preventivamente ogni archivio elettronico (file) acquisito attraverso qualsiasi supporto (es. Pen- drive) prima di trasferirlo su aree comuni della rete;

Agli utenti è fatto espresso divieto di influenzare negativamente la regolare operatività della Rete, interferire con la connettività altrui o con il funzionamento del sistema e quindi di:

a. 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, 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;

b. sostituirsi a qualcuno nell'uso dei sistemi, cercare di catturare password altrui o forzare password o comunicazioni criptate;
c. modificare le configurazioni impostate dall'amministratore di sistema;
d. limitare o negare l'accesso al sistema a utenti legittimi;
e. effettuare trasferimenti non autorizzati di informazioni (software, dati, ecc);
f. distruggere o alterare dati altrui;
g. usare l'anonimato o servirsi di risorse che consentano di restare anonimi.

Utilizzo di internet

L'accesso alla navigazione in Internet deve essere effettuato esclusivamente a mezzo della rete di istituto e solo per fini lavorativi o di studio. È tassativamente vietato l'utilizzo di modem personali. Gli utenti sono tenuti a utilizzare l'accesso ad internet in modo conforme a quanto stabilito dal presente Regolamento e quindi devono:

a. navigare in Internet in siti attinenti allo svolgimento delle mansioni assegnate;
b. registrarsi solo a siti con contenuti legati all'attività lavorativa;
c. partecipare a forum o utilizzare chat solo per motivi strettamente attinenti l'attività lavorativa;

Agli utenti è fatto espresso divieto di qualsiasi uso di internet che possa in qualche modo recare danno all'Istituto o a terzi e quindi di:

a. fare conoscere ad altri la password del proprio accesso, inclusi gli amministratori di sistema;
b. usare Internet per motivi personali;
c. servirsi dell'accesso Internet per attività in violazione del diritto d'autore o di altri diritti tutelati dalla normativa vigente;
d. accedere a siti pornografici, di intrattenimento, ecc.;
e. scaricare il software gratuiti dalla rete, salvo casi di comprovata utilità e previa autorizzazione in tal senso da parte del responsabile;
f. utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Winmx, e-Donkey, ecc.);
g. ascoltare la radio o guardare video o filmati utilizzando le risorse Internet;
h. effettuare transazioni finanziarie, operazioni di remote banking, acquisti on-line e simili, se non attinenti l'attività lavorativa o direttamente autorizzati dal responsabile del trattamento;
i. inviare fotografie, dati personali o di amici dalle postazioni Internet.

Utilizzo della posta elettronica

Gli utenti assegnatari di caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse e sono tenuti a utilizzarle in modo conforme a quanto stabilito dal presente Regolamento, quindi devono:

a. conservare la password nella massima riservatezza e con la massima diligenza;
b. mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
c. utilizzare tecniche per l'invio di comunicazioni a liste di distribuzione solo se istituzionali;
d. inoltrare al DSGA ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali con l'istituto e fare riferimento alle procedure in essere per la corrispondenza ordinaria;
e. utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
f. prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura e, dove possibile, preferire l'utilizzo di cartelle di rete condivise;

g. inviare preferibilmente file in formato PDF;
h. accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i file attachment di posta elettronica prima del loro utilizzo;
i. rispondere a e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
j. chiamare link contenuti all'interno di messaggi solo quando vi sia la comprovata sicurezza sul contenuto dei siti richiamati;
k. indicare la persona autorizzata ad aprire la posta o la persona che riceverà la posta in caso di assenza.

Agli utenti è fatto espresso divieto di qualsiasi uso della posta elettronica che possa in qualche modo recare danno all'Istituto o a terzi e quindi di:
a. prendere visione della posta altrui;
b. simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;
c. utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'istituto
d. trasmettere a mezzo posta elettronica dati sensibili, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati;
e. inviare tramite posta elettronica user-id, password, configurazioni della rete interna, indirizzi e nomi dei sistemi informatici;
f. utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mailing-list salvo diversa ed esplicita autorizzazione;
g. inviare o ricevere posta personale attraverso l'uso di un webmail;
h. inviare o accettare messaggi in formato html;
i. utilizzare il servizio di posta elettronica per inoltrare giochi, scherzi, barzellette, appelli e petizioni, messaggi tipo "catene" e altre e-mails che non siano di lavoro.

Utilizzo dei supporti magnetici

Gli utenti devono trattare con particolare cura i supporti magnetici (dischetti, nastri, DAT, chiavi USB, CD riscrivibili), in particolar modo a quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati ivi contenuti e quindi in particolare devono:
a. non utilizzare supporti rimovibili personali;
b. custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto;
c. consegnare i supporti magnetici riutilizzabili (dischetti, nastri, DAT, chiavi USB, CD riscrivibili) obsoleti all'Amministratore di Sistema per l'opportuna distruzione onde evitare che il loro contenuto possa essere, successivamente alla cancellazione, recuperato.

Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli e deve:
a. applicare al PC portatile le regole di utilizzo previste per i PC connessi in rete;
b. custodirlo con diligenza e in luogo protetto durante gli spostamenti;
c. rimuovere gli eventuali file elaborati sullo stesso prima della sua riconsegna.

Utilizzo delle stampanti e dei materiali di consumo

Stampanti e materiali di consumo in genere (carta, inchiostro, toner, floppy disk, supporti digitali come CD e DVD) possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi o utilizzi eccessivi.

Gli utenti devono effettuare la stampa dei dati solo se strettamente necessaria e ritirare prontamente dai vassoi delle stampanti comuni i fogli per impedire a persone non autorizzate di accedere alle stampe di documenti riservati.
Distruggere personalmente e sistematicamente le stampe che non servono più.

Utilizzo di telefonini e altre apparecchiature di registrazione di immagini e suoni

È fatto divieto assoluto di effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi, salvo

a. diversa disposizione esplicita del titolare del trattamento, da concordarsi di volta in volta e comunque sempre preventivamente al trattamento;
b. informazione preventiva degli interessati;
c. acquisizione del loro libero consenso, preventivo ed informato.

4. CONTROLLI

Il datore di lavoro, per esigenze organizzative, per garantire la sicurezza sul lavoro, per evitare reiterati comportamenti dolosi e illeciti può avvalersi legittimamente, nel rispetto dell'articolo 4 comma 2 dello Statuto dei lavoratori, di sistemi che consentano un controllo a distanza e determinano il trattamento di dati personali riferibili a singoli utenti.
Il datore di lavoro non può in alcun caso utilizzare detti sistemi per ricostruire l'attività del lavoratore tramite

- lettura e registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- memorizzazione sistematica delle pagine web visualizzate;
- lettura e registrazione dei caratteri inseriti dai lavoratori tramite tastiera o dispositivi analoghi;
- analisi occulta dei dispositivi per l'accesso a Internet o alla posta elettronica messi a disposizione dei dipendenti.

Le attività sull'uso del servizio di accesso ad Internet vengono automaticamente registrate attraverso il log di sistema ottenuti da un proxy server o da un altro strumento di registrazione delle informazioni. Analogamente sono parimenti suscettibili di controllo i servizi di posta elettronica. Tali file possono essere messi a disposizione dell'autorità giudiziaria in caso di accertata violazione della normativa vigente.
I dati contenuti nei log sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, produttive e di verifica della funzionalità dei sistemi di protezione e comunque non per più di un anno. Dopo tale periodo, il sistema cancella in modo automatico tali tracciati.
La riservatezza delle informazioni registrate è soggetta a quanto dettato dal D.Lgs. n. 196/2003, il trattamento dei dati avviene esclusivamente per fini istituzionali, per attività di monitoraggio e controllo e in forma anonima in modo tale da precludere l'identificazione degli utenti o delle loro attività. Le registrazioni possono essere utilizzate per fornire informazioni esclusivamente su:

- numero di utenti che visita ciascun sito o dominio, numero di pagine richieste e quantità di dati scaricati;
- numero di siti visitati da ciascun utente, quantità totale di dati scaricati, postazioni di lavoro utilizzate per la navigazione.

I dati personali contenuti nei log possono essere trattati tassativamente solo nelle seguenti ipotesi:

- per corrispondere ad eventuali richieste dell'autorità giudiziaria e della polizia postale;
- quando si verifichi un evento dannoso o una situazione di pericolo che richiede un immediato intervento;
- in caso di utilizzo anomalo che gli strumenti da parte degli utenti reiterato nonostante l'esplicito invito a ad attenersi a le istruzioni impartite.

Qualora i controlli evidenzino un utilizzo anomalo degli strumenti informatici dell'Istituto, il titolare del trattamento procede in forma graduata:

1. in via preliminare si eseguono controlli su dati aggregati, in forma anonima e si provvede ad un avviso generalizzato agli utenti;
2. se perdurano le anomalie si procede a controlli per tipologie di locali di utilizzo (uffici, aule, ecc.) o tipologie di utenti (ATA, docenti, studenti) e si procede con avvisi mirati alle categorie di utilizzatori;
3. ripetendosi l'anomalia, sarà lecito il controllo su base individuale e si procederà all'invio di avvisi individuali;
4. in caso di verificato e reiterato uso non conforme delle risorse informatiche il titolare del trattamento attiva il procedimento disciplinare
5. trattamenti in servizio proxy sono curati sono da personale tecnico incaricato del trattamento.

5. INFORMATIVA AGLI UTENTI

Il presente regolamento è messo a disposizione degli utenti, per la consultazione, sui mezzi di comunicazione interna utilizzati dall'Istituto e quindi sul sito web in formato PDF.
L'utente, qualora l'Istituto decidesse di perseguire, per fini legati alla sicurezza dell'intero sistema informativo, il controllo della posta e della navigazione in internet, viene informato degli strumenti e dei modi di trattamento effettuati prima che questo sia iniziato.

6. SANZIONI IN CASO DI MANCATO RISPETTO DEL REGOLAMENTO

La contravvenzione alle regole contenute nel presente regolamento da parte di un utente:
- può comportare 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;
- è perseguibile con provvedimenti disciplinari nelle forme con le modalità previste dall'Istituto per gli studenti, dai contratti di lavoro per i dipendenti e attraverso l'adozione degli atti di specifica competenza nel caso di personale non dipendente;
- può portare alle azioni civili e penali consentite.

L'utilizzo dei servizi di accesso ad Internet cessa o viene sospesa d'ufficio quando:
a. non sussiste più la condizione di dipendente/studente o l'autorizzazione al loro uso;
b. vi è il sospetto di manomissione dell'hardware o del software;
c. in caso di diffusione o comunicazione a terzi da parte del dipendente di password, codici di accesso ecc.;
d. in caso di accesso doloso a file o servizi non rientranti tra quelli autorizzati;
e. ogni qual volta sussistano ragionevoli evidenze di una violazione degli obblighi dell'utente che mette a rischio il sistema.

7. AGGIORNAMENTO E REVISIONE DEL REGOLAMENTO

Il presente Regolamento è soggetto a revisione con frequenza annuale e ogni qualvolta sia necessario un aggiornamento alla luce dell'esperienza, di nuove normative e dell'innovazione tecnologica.
Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento.
Le proposte verranno esaminate dal Titolare del trattamento in collaborazione con l'amministratore di sistema.

ALLEGATO B D.LGS 196 2003

Trattamenti con strumenti elettronici

Modalita' tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici e' consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o piu' credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati e' prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando e' prevista dal sistema di autenticazione, e' composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed e' modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave e' modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non puo' essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualita' che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici e' consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalita' con le quali il titolare puo' assicurare la disponibilita' di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessita' di operativita' e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali e'

organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso e' utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, e' verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati puo' essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilita' di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento e' almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilita' nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrita' e la disponibilita' dei dati, nonche' la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilita';

19.5. la descrizione dei criteri e delle modalita' per il ripristino della disponibilita' dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali piu' rilevanti in rapporto alle relative attivita', delle responsabilita' che ne derivano e delle modalita' per aggiornarsi sulle misure minime adottate dal titolare. La formazione e' programmata gia' al momento dell'ingresso in servizio, nonche' in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformita' al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalita' di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identita' genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico e' cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformita' alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta,

dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici
Modalita' tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati puo' essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari e' controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.