ISTITUTO SUPERIORE SECONDO GRADO
"I.S.I.S di Quarto"
Via Vaiani, 44 - 80010 Quarto (Napoli) Tel. 081/8060529 – fax 081/8061330
Codice Meccanografico NAIS03700Q C.F:9601900633
e-mail: nais03700q@istruzione.it
DISTRETTO SCOLASTICO 025

DISCIPLINARE INTERNO PER L'UTILIZZO DELLE STRUMENTAZIONI INFORMATICHE, DELLE RETI INTERNET E DELLA POSTA ELETTRONICA DA PARTE DEL PERSONALE E DEGLI STUDENTI.

1.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 l'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 rischi possibili e conseguenti effetti:

Attività	Rischio	Motivazione	Possibile effetto
Manutenzione di periferiche hardware interne (schede video, memoria, etc.)	Alto	Possono essere danneggiati componenti interni e il PC	Danneggiamento dei PC
Manutenzione di periferiche hardware esterne (tastiere, mouse, etc.)	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 informatca 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, etc.)	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 dell rete informatica interna.
Accesso alla rete effettuato da PC di proprietà dell'utente	Alto	Acessi 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 oinformatica 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)contenente 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 direttamente 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 all'amministratore di sistema il compito di sovrintendere alle risorse informatiche dell'Istituto assegnandogli in maniera esclusiva le seguenti attività:

Avrà il compito di generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i codici di accesso personali da assegnare agli incaricati del trattamento dati, nel rispetto delle massime misure di sicurezza.

Dovrà, inoltre, adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza nel rispetto di quanto dettato dal Dlgs 196/2003 ed utilizzando le conoscenze acquisite in base al progresso tecnico software e hardware.

L'incaricato ha il compito di controllare periodicamente l'efficienza dei sistemi tecnici adottati e di redigere un apposito verbale, da consegnare al titolare o al responsabile, riportante i nominativi dei partecipanti al controllo, i riscontri e le verifiche effettuate, i parametri adottati e gli accorgimenti proposti per migliorare la sicurezza.

L'incaricato prenderà tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up.

Dovrà assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro.

Fare in modo che sia prevista la disattivazione dei codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei codici identificativi personali per oltre 6 mesi.

E' compito dell'amministratore di sistema indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego.

Sarà inoltre custode delle parole chiave o password per l'accesso dei dati archiviati nei sistemi di elaborazione dei dati.

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 d'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 essere 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 ad 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.

PROCEDURE DI GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE

a. E' 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 passwordo provvisoria che l'utente dovrà cambiare al primo accesso.
b. Per scegliere la nuova aprola 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 dei congiunti (coniuge, figli, genitori), di animali domestici o date di nascita, numeri 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 copn 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 una busta chiusa con data e firma dell'incaricato apposte sul lembo di chiusura, perché ne curi la conservazione.
e. E' necessario curare la conservazione della propria parola chiave e bisogna evitare di comunicarla ad altri, di trascriverla su sopporti (agenda, post-it etc.) che siano accessibili ad altri o di consentire che qualcuno sbirci quello che si sta battendo sulla tastiera quando viene immessa la password.
f. Nel caso si sospetti che la password abbia perso la segretezza essa deve essere immediatamente sostituta, dandone comunicazione scritta all'incaricato della custodia delle Password.

Utilizzo di internet

La navigazione di 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.

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, coin cancellazione dei files 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 files o software)

DIRITTI E RESPONSABILITA' DEI DIPENDENTI

Per assicurare la tutela dei diritti, delle libertà fondamentali e delle 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.

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 portare 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.

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 sceen saver e la relativa password;
b. conservare la password nella massima riservatezza e diligenza;
c. non inserire password locali che non rendano accessibili il computer agli amministratori di rete se non esplicitamente autorizzato dall'amministratore di sistema;
d. non utilizzare criptosistemi o qualsiasi altro programma di sicurezza crittografica non previste esplicitamente dal servizio informatico dell'istituto;
e. non modificare la configurazione hardware e software del proprio PC, se non esplicitamente autorizzati dall'amministratore di sistema;
f. non rimuovere, danneggiare o asportare componenti hardware;
g. non installare sul proprio PC dispositivi hardware personali (modem, schede audio,masterizzatori, pen drive, dischi esterni, i-pod, telefoni, etc.), salvo specifica autorizzazione in tal senso da parte del responsabili;
h. non installare autonomamente programmi informatici, se non esplicitamente autorizzati dall'ammministratore di sistema;
i. 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;

l .prestare la massima attenzione ai supporti di origine esterna (es. pen drive), verificando preventivamente tramite il programma antivirus ogni file acquisito attraverso qualsiasi supporto e avvertendo immediatamente l’amministratore di sistema nel caso vengono 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 riguardo 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 noin 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, coin cancellazione dei files o inutili ed evitare un'archiviazione ridondante;

c. verificare preventivamente ogni archivio elettronico (file) acquisito attraverso qualsiasi supporto (es. pen drive) prima di trasferirolo su aree comuni della rete;

Agli utenti è fatto espresso divieto di influenzare negativamente la regolare attività 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 agli utenti legittimi;

e. effettuare trasferimenti non autorizzati di informazioni (software, dati, etc.)

f. distruggere o alterare dati altrui;

g. usare l'anonimato o servirsi di risorse che consentono di restare anonimi.

Utilizzo di internet

L'accesso alla navigazione in Internet deve essere effettuato esclusivamente a mezzo della rete di istituto e solo ai fini lavorativi o di studio . E' tassativamente vietato l'utilizzo di modem personali.

Gli utenti sono tenuti ad 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, etc. ;

e. scaricare software gratuiti dalla rete, salvo casi di comprovata utilità e previa autorizzazione in tal sensoda parte del responsabili;

f. utilizzare programmi per la condivisione e lo scambio di file in modalità peer to peer (Napster, Emule, Winmex, e-Donkey, etc.);

g. ascoltare la radio o guardare video o filmati utilizzando le risorse internet;

h. effettuare transazioni finanziarie, operazioni di remote bancking, 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 sono responsabili del corretto utilizzo delle caselle di posta elettronica istituzionali e sono tenuti ad 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 comunicazione a liste di distribuzione solo se istituzionali;

d. utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;

e. 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;

f. inviare preferibilmente files in formato PDF;

g. accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i files attachment di posta elettronica prima del loro utilizzo;

h. rispondere a e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;

i. chiamare link contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto di siti richiamati;

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 quidi di:

a. utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'istituto;

b. 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;

c. inviare tramite posta elettronica user-id, password, configurazioni della rete interna , indirizzi e nomi dei sistemi informatici;

d. 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;

e. inviare o ricevere posta personale attraverso l'uso di un webmail;

f. inviare o accettare messaggio in formato html;

g. 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 particol modo devono:

a. 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, 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 assegnatigli 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;rimuovere gli eventuali files elaborati sullo stesso prima della sua riconsegna.

Utilizzo delle stampanti e dei materiali di consumo

Stampanti e materiali di consumo in genere (carte, inchiostro, toner, floppy disck, supporti digitali cone CD e DVD) possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi e 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 ed altre apparecchiature di registrazione di immagini e suoni

E' 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 agli 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 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 di messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- memorizzare sistematica delle pagine web visualizzate;
- lettura e registrazione dei caratteri inseriti dal lavoratore 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 altro strumento di registrazione delle informazioni. Analogamente sono parimenti suscettibili di controllo i servizi di posta elettronica. Tali files possono essere messi a disposizione ndell'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 di verifica della funzionalità dei sistemi di protezione.

La riservatezza delle informazioni registrate e 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'isentificazione 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 dati scaricati;
- numero dei 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 degli strumenti da parte degli utenti reiterato nonostante l'esplicito invito ad attenersi alle istruzioni impartite.

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

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

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 pubblicato all'albo e sul sito web dell'istituto.

L'utente,qualora l'istituto decidesse di perseguire, per fini legati alla sicurezza dell'intero sistema informatico, il controllo della posta e della navigazione in internet, viene informato degli strumenti e dei modi di trattamento effetuati prima che questi 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 autorizzazione ad accedere alla rete informatica ed ai servizi/programmi autorizzati, fatte salve le sanzioni più gravi previste dall'istituto per gli studenti, dai contratti di lavoro per i dipendenti e attraverso l'adozione degli atti di specifica competenza nel caso del 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, di codici di accesso etc.;
d. in caso di accesso doloso a files o servizi non rientranti tra quelli autorizzati;
e. ogni qualvolta 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 il responsabile del trattamento e dell'amministratore di sistema.

41