ISTITUTO DI ISTRUZIONE
SECONDARIA SUPERIORE

"LUIGI VANVITELLI" *LIONI (AV)*

REGOLAMENTO SICUREZZA INFORMATICA

PER UN CORRETTO UTILIZZO DELLE STRUMENTAZIONI INFORMATICHE, DELLA RETE INTERNET E DELLA POSTA ELETTRONICA DA PARTE DEL PERSONALE E DEGLI STUDENTI

Delibera del Consiglio di Istituto del 10 settembre 2020

Oggetto e ambito di applicazione

Il presente regolamento disciplina le modalità di accesso, di uso della rete informatica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire all'interno e all'esterno dell'Istituzione scolastica.
Le risorse infrastrutturali sono le componenti hardware/software e gli apparati elettronici collegati alla rete informatica della scuola. Il patrimonio informativo è l'insieme delle banche dati in formato digitale ed in generale tutti i documenti prodotti tramite l'utilizzo dei suddetti apparati.
Il presente regolamento si applica a tutti gli utenti interni ed esterni che sono autorizzati ad accedere alla rete della scuola. Per utenti interni si intendono tutti gli amministrativi, i docenti e i collaboratori scolastici. Per utenti esterni si intendono le ditte fornitrici di software che effettuano attività di manutenzione limitatamente alle applicazioni di loro competenza, enti esterni autorizzati da apposite convenzioni all'accesso a specifiche banche dati con le modalità stabilite dalle stesse e i collaboratori esterni.

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, sotto il profilo sia civile sia penale, del corretto uso delle Risorse informatiche, dei Servizi e dei programmi ai quali ha accesso e dei dati che tratta. Spetta ai docenti illustrare agli studenti i contenuti del presente regolamento e vigilare affinché gli studenti loro affidati lo rispettino.

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.

Utilizzo dei personal computer, tablet o altro device

Gli utenti utilizzano per il proprio lavoro soltanto computer, tablet o device 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;
e. non modificare la configurazione *hardware* e *software* del PC, se non a seguito di esplicita autorizzazione;
f. non rimuovere, danneggiare o asportare componenti *hardware;*
g. non installare sul PC dispositivi *hardware* personali (modem, schede audio, masterizzatori, *pendrive*, dischi esterni, *i-pod*, telefoni, ecc.), salvo specifica autorizzazione in tal senso da parte del responsabile;
h. non installare autonomamente programmi informatici, se non esplicitamente autorizzati dall'Amministratore 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. 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;
l. non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
m. 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 al server, ad Internet e ai servizi di posta elettronica;

n. 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 due mesi) alla pulizia degli archivi, con cancellazione dei *file* obsoleti o inutili ed evitare un'archiviazione eccessiva;
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 *file* 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.

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:
1. fare conoscere ad altri la password del proprio accesso, inclusi gli amministratori di sistema;
2. usare Internet per motivi personali;
3. servirsi dell'accesso Internet per attività in violazione del diritto d'autore o di altri diritti tutelati dalla normativa vigente;
4. scaricare il software gratuiti dalla rete, salvo casi di comprovata utilità e previa

autorizzazione in tal senso da parte del responsabile;
5. guardare video o filmati utilizzando le risorse Internet se non per motivi attinenti il lavoro;
6. 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;
7. 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 a 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 mittenti 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;

Utilizzo delle password

Le password di ingresso alla rete, di accesso ai programmi e dello screensaver, sono previste ed attribuite dall'Incaricato della custodia delle Password, ovvero dal responsabile all'impiego delle risorse informatiche.
È necessario procedere alla modifica della password a cura del responsabile del trattamento al primo utilizzo e, successivamente, con scansione trimestrale (come previsto dal punto 5 del disciplinare tecnico allegato al Codice della privacy, D.lgs. n.196/2003) con contestuale comunicazione all'Incaricato della custodia delle Password.
Qualora la password non venga autonomamente variata dall'incaricato entro i termini massimi, l'utente verrà automaticamente disabilitato.
Sarà quindi necessario rivolgersi all'Amministratore di Sistema dell'Istituto o al Responsabile, il quale provvederà a riabilitare l'utente ed assegnargli una password provvisoria che l'utente dovrà cambiare al primo accesso.
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 devono 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, al Responsabile.

Utilizzo dei supporti magnetici

Gli utenti devono trattare con particolare cura i supporti magnetici (chiavi USB, CD riscrivibili,..), in particolar modo 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 per il trasferimento dei dati sensibili;
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 obsoleti al Responsabile 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 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.
Si dovranno 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.

Amministratore di sistema – Responsabile all'impiego delle risorse informatiche

L'Amministratore di Sistema e il Responsabile all'impiego delle risorse informatiche sono i soggetti cui è conferito il compito di sovrintendere alle risorse informatiche dell'Istituto e a cui sono consentite in maniera esclusiva le seguenti attività:
a) Gestire l'hardware e il software di tutte le strutture tecniche informatiche di appartenenza dell'Istituto, collegate in rete o meno;
b) Gestire esecutivamente (creazione, attivazione, disattivazione e tutte le relative attività amministrative) gli account di rete e i relativi privilegi di accesso alle risorse, assegnati agli utenti della Rete Informatica istituzionale, secondo le direttive impartite dal Titolare;
c) Monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
d) Creare, modificare, rimuovere o utilizzare qualunque account o privilegio, attesa l'autorizzazione del Titolare, solo se rientrante nelle 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) Rimuovere programmi software dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
f) Rimuovere componenti hardware dalle risorse informatiche assegnate agli utenti, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
g) Utilizzare le credenziali di accesso di amministrazione del sistema, o l'account di un utente tramite re-inizializzazione della relativa password, per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di prolungata assenza, non tracciabilità o impedimento dello stesso. Tale utilizzo deve essere esplicitamente richiesto dal Titolare per l'utente assente o impedito, e deve essere limitato al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

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 gli utenti interni perseverassero nell'uso ed abuso degli strumenti elettronici a loro disposizione, il datore di lavoro è autorizzato a procedere con controlli prima sull'ufficio ed, infine, sul gruppo di lavoro; solo a questo punto, ripetendosi l'anomalia, sarà lecito il controllo su base individuale.

Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Il presente Regolamento è soggetto a revisione con frequenza annuale o in caso di variazioni della normativa vigente.