Ministero dell'Istruzione, dell'Università e della Ricerca Ufficio Scolastico Regionale per la Sicilia

C.P.I.A. CT1 CATANIA

Centro Provinciale per l'Istruzione degli Adulti

Via Velletri, 28 – 95126 CATANIA

Cod.Fisc. 93203370874 - Cod.Mecc. CTMM150008

Tel 0958259050 -

e-mail: ctmm150008@istruzione.it pec.: ctmm150008@pec.istruzione.it

CPIA DI CATANIA 1 - -CATANIA
Prot. 0006475 del 14/10/2019
01-04 (Uscita)

REGOLAMENTO ORGANIZZATIVO PER L'UTILIZZO DEI BENI LAVORATIVI, DEGLI STRUMENTI INFORMATICI, DI INTERNET E DELLA POSTA ELETTRONICA

Mod. R1.4 Rev. 2019

Le presenti regole di sicurezza hanno valenza per l'intera struttura organizzativa e si pongono l'obiettivo di fornire agli utenti idonee misure di sicurezza e linee di comportamento adeguate a un utilizzo corretto e conforme alla politica organizzativa degli strumenti elettronici, della posta elettronica istituzionale, la navigazione in internet e l'uso degli applicativi istituzionali quali a titolo esemplificativo e non esaustivo:

- SOGI
- PORTALE ARGO
- SIDI
- PORTALI PUBBLICI (ag. Entrate, Inps, PCC, ANAC, CIG, DURC, sito istituto, ecc.)

A tutti gli utenti è richiesto di attenersi scrupolosamente alle leggi vigenti in termini di protezione dei dati personali quali il Reg. UE 2016/679 ed il D.Lgs. 101/18, compresa la Legge 547/93 ed il D.Lgs. 231/01 sulla criminalità informatica per quanto concerne abusi, danneggiamenti e alterazioni di software, falsi e frodi informatiche, spionaggio informatico, intercettazione ed uso abusivo di codici d'accesso, uso improprio di informazioni ottenute con mezzi illeciti.
Copia del presente Regolamento viene letto in apposita riunione formativa e consegnata a ciascun Autorizzato all'atto dell'assunzione e/o ad inizio attività. L'osservanza delle disposizioni regolate dalla normativa sopra citata deve considerarsi parte essenziale delle obbligazioni contrattuali dei dipendenti ai sensi e per gli effetti di cui all'art. 2104 codice civile. L'inosservanza delle norme sulla privacy può comportare inoltre sanzioni di natura civile e penale per l'Autorizzato e per l'organizzazione, per cui si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate.

Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'Organizzazione.
È opportuno evidenziare che nessuna guida operativa, per quanto dettagliata, potrà mai sostituire le intuizioni dettate dal buon senso e dal rispetto della dignità umana, in modo particolare quando il trattamento dei dati coinvolge dati che attengono strettamente la sfera personale dell'interessato.
Le presenti istruzioni si applicano:
- a tutti i lavoratori dipendenti e a tutti i collaboratori del Titolare (l'Organizzazione o l'Istituto) a prescindere dal rapporto contrattuale con la stessa intrattenuta (lavoratori somministrati, collaboratori a progetto, agenti, stagisti, consulenti, agenzie, call center esterno, ecc.) che si trovano a operare sui dati personali di cui l'Istituto stesso è Titolare (di seguito "Autorizzato");
- a tutte le attività o comportamenti comunque connessi all'utilizzo della rete Internet, della posta elettronica e degli applicativi on-line sopra menzionati, mediante strumentazione dell'istituto o di terze parti autorizzate all'uso dell'infrastruttura dell'istituto (con apposito contratto a Responsabile esterno al trattamento).

USO DI ATTREZZATURE E DI BENI DELL'ISTITUTO
Di seguito vengono descritte le norme a cui gli Autorizzati devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali riferiti sia a persone fisiche che giuridiche.

Ministero dell'Istruzione, dell'Università e della Ricerca Ufficio Scolastico Regionale per la Sicilia

C.P.I.A. CT1 CATANIA

Centro Provinciale per l'Istruzione degli Adulti

Via Velletri, 28 – 95126 CATANIA

Cod.Fisc. 93203370874 - Cod.Mecc. CTMM150008

Tel 0958259050 -

e-mail: ctmm150008@istruzione.it pec.: ctmm150008@pec.istruzione.it

Preliminarmente va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, l'Autorizzato deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy, nonché la riservatezza dei dati considerati riservati per il Titolare:

- tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
- le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;
- in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie (es. blocco del pc) affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;
- non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal Titolare;
- devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;
- deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi;
- quando si effettua un trattamento occorre essere autorizzati dal Titolare all'attività in questione.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi del trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

Nei successivi paragrafi si riportano le norme che gli Autorizzati devono adottare nel trattamento dei dati, sia in formato elettronico che cartaceo.

Gli altri compiti ed istruzioni comprendono:

- identificazione dell'interessato: al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di

identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;

- raccolta: prima di procedere alla raccolta dei dati personali deve essere fornita l'informativa all'interessato o alla persona presso cui si raccolgono i dati (sarà cura del Titolare decidere le modalità per adempiere a questo obbligo); occorre procedere alla raccolta dei dati con la massima cura, verificandone l'esattezza, la pertinenza, la completezza e la non eccedenza rispetto alle finalità del trattamento in conformità a quanto previsto dalla legge e dai regolamenti, seguendo le istruzioni del Titolare del trattamento;
- registrazione: nel caso di inserimento in uno dei sistemi informativi dell'istituto, è necessario operare con la massima attenzione al fine di non omettere dati o inserire dati non corretti; durante tali operazioni fare particolare attenzione a non lasciare dischetti, fogli, cartelle e quant'altro a disposizione di estranei;
- conservazione: i documenti o gli atti che contengono categorie particolari di dati vanno conservati in archivi ad accesso controllato. È quindi necessario garantire che armadi, schedari e contenitori siano muniti di serratura e che l'Autorizzato del trattamento, che riceva interessati ed utenti, sia sempre presente nella propria stanza o luogo di lavoro avendo cura di evitare che le informazioni trattate possano essere visualizzate e rese conoscibili a terzi. Sarà cura del Titolare del trattamento adottare i provvedimenti necessari affinché venga escluso un accesso ad archivi ed a dati da parte di soggetti che non siano Autorizzati al trattamento;
- utilizzo: i dati possono essere utilizzati solo da coloro che sono stati espressamente autorizzati al trattamento. L'utilizzo dei dati deve avvenire solo per scopi determinati, espressi e legittimi, avendo cura di evitare un utilizzo per scopi che non coincidano o che non siano compatibili con quelli istituzionali della Istituto in riferimento alle attività affidate e di competenza dell'unità di trattamento di appartenenza;
- limitazione: questa operazione può essere conseguenza di una espressa richiesta da parte dell'interessato ovvero può essere ordinata direttamente dal Garante per la protezione dei dati personali;
- comunicazione: con tale espressione, secondo quanto previsto dalla legge, si intende *"il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione"*. Ciò che caratterizza l'operazione di comunicazione è il fatto che, considerato il rapporto diretto tra Titolare (la Istituto) e l'interessato (ad esempio un cittadino utente, un dipendente o un'impresa), un soggetto determinato (in posizione di terzietà rispetto a questo rapporto bilaterale) possa in qualunque forma conoscere dati personali riferiti all'interessato medesimo;
- diffusione: per diffusione si intende *"il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione"*. È espressamente vietata la diffusione di dati personali idonei a rivelare lo stato di salute;

Utilizzo di Computer, Periferiche, Materiale Di Consumo vario.

La postazione di lavoro, indipendentemente dal fatto che si tratti di un computer portatile, di un computer desktop, di un telefono "smartphone" o di un tablet, deve essere:

- utilizzata solo per scopi legati alla propria attività lavorativa;
- utilizzata in modo esclusivo per un solo Autorizzato (salvo diverse ed opportune partizioni dei dischi rigidi, opportunamente previste e separate);
- protetta, evitando che terzi possano accedere ai dati che si stanno trattando.

Ministero dell'Istruzione, dell'Università e della Ricerca Ufficio Scolastico Regionale per la Sicilia

C.P.I.A. CT1 CATANIA

Centro Provinciale per l'Istruzione degli Adulti

Via Velletri, 28 – 95126 CATANIA

Cod.Fisc. 93203370874 - Cod.Mecc. CTMM150008

Tel 0958259050 -

e-mail: ctmm150008@istruzione.it pec.: ctmm150008@pec.istruzione.it

Occorre, inoltre, precisare che è dovere dell'Autorizzato:

- Non utilizzare risorse informatiche private (PC, periferiche, token, pen drive ecc.) salvo apposita autorizzazione del Titolare del trattamento;
- Non installare autonomamente programmi provenienti dall'esterno, salvo previa autorizzazione esplicita del Titolare del Trattamento, in quanto sussiste il grave pericolo di portare virus informatici e/o di alterare la stabilità delle applicazioni dell'elaboratore;
- Non utilizzare programmi diversi da quelli distribuiti e installati ufficialmente dall'Amministratore di Sistema. L'inosservanza di questa disposizione, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre la Istituto a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D.Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore (copyright);
- Non modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell'Amministratore di Sistema;
- Non lasciare sulla scrivania informazioni riservate e su qualunque supporto esse siano archiviate (carta, CD, dischetti, pen drive, ecc.);
- Richiamare le funzioni di sicurezza del sistema operativo (con la sequenza dei tasti CTRL+ALT+CANC) ed assicurarsi della attivazione della funzione "Blocca" in caso di abbandono momentaneo del proprio PC e, in alternativa, impostare lo screen saver con password in modo che si attivi dopo al massimo 5 minuti di inattività;
- Non lasciare il computer portatile incustodito sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro, o durante riunioni lontane dalla propria postazione);
- Non lasciare incustoditi cellulari o tablet;
- Non utilizzare fax e/o telefono per trasmettere informazioni riservate e personali se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario o se esso non è legittimato a riceverle. Si consiglia, qualora si nutrano dubbi sull'identità di chi è dall'altra parte dell'apparecchio, di richiedere identità e qualifica dell'interlocutore, al fine di richiamarlo successivamente per avere certezza sulla sua identità;
- Al verificarsi di un malfunzionamento del PC, che può far sospettare la presenza di un virus informatico, è bene sospendere ogni operazione sul PC, evitando di lavorare con il sistema infetto e contattare immediatamente l'Ufficio IT.

Coloro che provvedono all'acquisizione in formato digitale della documentazione cartacea devono verificare

che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile al fine di evitare confusione di dati;
La documentazione contenente categorie particolari di dati deve essere trasferita, anche all'interno della struttura, in busta chiusa (carpetta), in modo da assicurare la protezione della riservatezza sia del documento, sia dei dati in esso contenuti. Per dare garanzia della non apertura della busta e della integrità del contenuto, sarebbe opportuno che i lembi della busta fossero sigillati e firmati. In alternativa è comunque opportuno piegare il documento spillandone i lati;

Istruzioni In Tema Di Sicurezza Degli Strumenti Elettronici

Rete dell'istituto

Per l'accesso alla rete ciascun utente deve essere in possesso delle specifiche credenziali di autenticazione. Le cartelle presenti nei server sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte del Titolare. Gli operatori dell'IT possono in qualunque momento procedere alla rimozione di ogni file o applicazione che potrebbe risultare pericolosa per la sicurezza, sia sui PC degli Autorizzati che sulle unità di rete.

Gestione delle password

Ciascun Autorizzato accede alla rete e alle sue risorse utilizzando delle credenziali costituite da un nome utente ed una password.
Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dall'Amministratore di Sistema. È necessario procedere alla modifica della password a cura dell'Autorizzato al trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di categorie particolari di dati, la frequenza di modifica deve essere ridotta a tre mesi (*n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al custode; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'Autorizzato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento)*
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'Autorizzato (per esempio, la propria data di nascita).
La password deve essere immediatamente sostituita, dandone comunicazione al Titolare, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'Autorizzato venisse a conoscenza delle password di altro Autorizzato, è tenuto a darne immediata notizia al Titolare o persona dalla stessa incaricata.

Le postazioni dell'istituto sono dotate di software antivirus, installato dal personale dell'IT, che ne configura la modalità di aggiornamento automatico.
L'operatore che verifica che la postazione dalla quale utilizza la rete pubblica Internet non è dotata di

programma antivirus, o che questo non è aggiornato, deve segnalare all'Amministratore di Sistema tale situazione.

Salvo che non sia previsto un sistema di salvataggio di dati personali automatico ovvero centralizzato, occorre procedere, con cadenza almeno settimanale, alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento, utilizzando gli apparati a disposizione, per poi consegnare i supporti contenenti le copie di salvataggio al soggetto nominato ed Autorizzato alla conservazione. In alternativa, si possono riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati.

Strumenti portatili

Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa. Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono illustrate le ulteriori precauzioni da adottare nell'uso dei dispositivi portatili:

conservare lo strumento in un luogo sicuro alla fine della giornata lavorativa;

non lasciare mai incustodito l'elaboratore in caso di utilizzo in ambito esterno alla Istituto;

in caso di furto di un PC portatile avvertire tempestivamente l'Ufficio IT, che darà le opportune indicazioni;

essere sempre ben consapevole delle informazioni archiviate sul portatile il quale è maggiormente soggetto a furto o smarrimento rispetto alla postazione fissa;

operare sempre nella massima riservatezza quando si utilizza il PC portatile in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti.

Dispositivi di archiviazione

Tutti i supporti riutilizzabili (pen drive, dischi esterni usb, schede di memoria, ecc.) contenenti dati sensibili e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. I supporti portatili contenenti dati sensibili e giudiziari devono essere custoditi in archivi chiusi a chiave.

ISTRUZIONI PER GLI ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione dei sistemi informatici che sono nominati Responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:

- Effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
- gestire le credenziali di autenticazione dei soggetti autorizzati del trattamento su indicazione dell'Amministratore di Sistema;

• gestire i profili di autorizzazione degli Autorizzati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di Sistema;
• provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane (fare procedura affinché licenziamenti/dimissioni vengano comunicati ad IT. Pianificare verifiche semestrali) e su indicazione dell'Amministratore di Sistema;
• custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;
L'accesso degli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.
A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:
• Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare file già esistenti ma creare file di prova.
• Nel caso si renda strettamente necessario accedere a file contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.
• Per effettuare operazioni di manutenzione sui database dell'istituto che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
• Devono inoltre essere adottate misure di sicurezza idonee previste dal Reg. UE 2016/679 in materia di protezione dei dati personali;
• E' necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.
• Tutti i dati personali contenuti nei data base devono essere protetti da password;
• Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli Autorizzati, attenersi alle indicazioni previste contrattualmente e secondo la normativa vigente.
• Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'Amministratore di Sistema o provvedere, in collaborazione con l'Amministratore di Sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;
• L'Amministratore di Sistema ha facoltà, in qualunque momento, di controllare e verificare l'operato degli addetti alla manutenzione;
• Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'autorizzato, il quale provvederà a cambiarla al termine delle operazioni di manutenzione;
• l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è

consentito unicamente previo inserimento di password e ID;

• è assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla Istituto, se non previa espressa comunicazione scritta;

• Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali, deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni in materia di misure minime di sicurezza.

---ooo0ooo---

INTERNET E POSTA ELETTRONICA

Gli strumenti di comunicazione telematica (Internet e posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative.

Sono vietati comportamenti che possano arrecare danno alla Istituto.

In particolare, l'Autorizzato dovrà osservare le seguenti:

1) è consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate;
2) non è consentito scaricare software gratuiti (freeware o shareware) prelevati da siti Internet;
3) non è consentita la registrazione a siti internet o partecipare a Forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa;
4) non è consentito l'utilizzo di instant messaging a meno che autorizzate dall'Ufficio IT;
5) è consentito solo l'utilizzo dei programmi ufficialmente installati dall'Ufficio IT;
6) è vietato installare autonomamente programmi, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti, di violare la legge sul diritto d'autore, non disponendo delle apposite licenze d'uso acquistate dall'Istituto;
7) è vietato modificare le caratteristiche impostate sulle dotazioni od installare dispositivi di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, etc.), collegare alla rete dell'istituto qualsiasi apparecchiatura (ad es. switch, hub, apparati di memorizzazione di rete, etc.), effettuare collegamenti verso l'esterno di qualsiasi tipo (ad es. tramite modem o simili, etc.) utilizzando un pc che sia contemporaneamente collegato alla rete Dell'istituto (creando così un collegamento tra la rete Dell'istituto interna e la rete esterna);
8) va sempre prestata la massima attenzione nell'utilizzo dei supporti di origine esterna (per es. pen drive USB, dischi esterni, ecc.), avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus.
9) Occorre separare la rete wifi utilizzata dagli ospiti rispetto alla rete dell'istituto. Allo stesso modo, l'accesso alla rete wifi da parte dei dipendenti, con i propri dispositivi personali, deve essere separato rispetto alla

rete dell'istituto.

Il titolare assegna l'utilizzo della posta elettronica a soggetti autorizzati all'uso di questo strumento. Gli indirizzi possono essere assegnati per funzione e/o nominativi. Inoltre l'accesso alle caselle di posta può essere condiviso fra più soggetti autorizzati (es. amministrazione@titolare.it, info@istituto.it , nome.cognome@titolare.it.).
I soggetti che sono autorizzati all'uso di uno specifico indirizzo di posta Dell'istituto devono considerarsi edotti del fatto che la casella di posta elettronica utilizzata è uno "strumento Dell'istituto".
Per questo motivo l'accesso non potrà considerarsi esclusivo e, conseguentemente, i contenuti potranno essere conosciuti da tutti i soggetti che da atto di nomina o per analogia di funzione saranno autorizzati ad utilizzare la stessa casella di posta elettronica per il raggiungimento dei medesimi fini dell'istituto.
L'uso della posta elettronica per la trasmissione, l'elaborazione, l'archiviazione di informazioni sia verso utenti interni alla Istituto sia verso utenti esterni, rappresenta un'esigenza professionale che richiede il rispetto dei seguenti principi:

- tutela dell'immagine della Istituto;
- rispetto dell'etica dell'ambiente di lavoro;
- osservanza della riservatezza da parte dei dipendenti;
- correttezza dei rapporti tra colleghi e con terzi;
- rispetto delle normative vigenti.

Nell'utilizzo della posta elettronica ciascun Autorizzato deve tenere in debito conto che i soggetti esterni possono attribuire carattere istituzionale alla corrispondenza ricevuta da dipendenti della Istituto.
Pertanto, si deve prestare particolare attenzione agli eventuali impegni contrattuali e precontrattuali contenuti nei messaggi. Inoltre, la formulazione dei messaggi deve far uso di un linguaggio appropriato, corretto e rispettoso, che tuteli la dignità delle persone, l'immagine e la reputazione dell'istituto.

L'Istituto formula inoltre le seguenti regole di comportamento a cui gli utenti devono attenersi.
L'Istituto dispone dell'uso di posta elettronica del tipo "ufficio" *@titolare.it . Il servizio di posta elettronica attivato è pertanto direttamente riferibile alla Istituto ed è dalla stessa attivato al solo scopo dell'utilizzo dell'istituto. Le credenziali di accesso alle singole caselle di posta elettronica dell'istituto saranno dunque nella disponibilità sia dei singoli soggetti autorizzati, come indicato al successivo punto 4, che del Titolare del trattamento dati effettuato attraverso lo strumento di posta elettronica dell'istituto.
I soggetti autorizzati dovranno adoperare la massima diligenza nel custodire dette credenziali di accesso e non potranno modificarli, se non previa autorizzazione da parte del Titolare.
Per utilizzo dell'istituto deve intendersi qualunque operazione di ricezione e/o trasmissione di contenuti in formato elettronico relativi, in modo diretto o indiretto, all'attività svolta dalla organizzazione (in via meramente esemplificativa e non esaustiva si indicano: preventivi, offerte, comunicazioni con clienti, comunicazioni di trattative precontrattuali).
Deve considerarsi non autorizzato, e dunque illegittimo, l'utilizzo del servizio di posta elettronica, come sopra descritto, per uso personale da parte di dipendenti e collaboratori.
L'utente deve utilizzare la propria casella di posta elettronica solo per attività connesse alla propria mansione e per altre attività strumentali o correlate ai fini istituzionali, nel rispetto di quanto disposto

dalla normativa vigente e comunque senza recar danno o pregiudizio all'Organizzazione medesima o a terzi.

L'utente non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato, messaggi che contengano o rimandino a:

- Pubblicità non istituzionale, manifesta o occulta;
- Comunicazioni commerciali private;
- Comunicazioni di propaganda politica esterna all'Organizzazione;
- Materiale pornografico o simile;
- Materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
- Materiale che violi la normativa sulla privacy;
- Contenuti o materiali che violino i diritti di proprietà di terzi;
- Contenuti diffamatori o palesemente offensivi;
- Altri contenuti illegali.

L'elenco che precede va considerato in via esemplificativa e non esaustiva.

Gli utenti, nella consultazione della posta, devono adottare comportamenti che non pregiudichino la sicurezza informatica dell'istituto.

In particolare, gli utenti devono:

- prestare molta attenzione a messaggi o allegati che provengono da mittenti sconosciuti o poco attendibili e, in caso non si individui il mittente, non aprirli;
- non aprire allegati di messaggi di posta con estensione eseguibile (ad es.: .exe, .bat, .com, .iso);
- assicurarsi che i sistemi di sicurezza del sistema operativo siano operativi ed efficienti;
- disattivare l'anteprima automatica dei messaggi;
- disattivare l'anteprima automatica dei contenuti dei file allegati.

Gli utenti sono tenuti alla regolare consultazione della propria casella.

Responsabilità dell'Utente

L'utente si assume ogni responsabilità penale e civile e il carico di ogni eventuale onere derivante dall'uso improprio del servizio, esonerando, contestualmente, l'Organizzazione da ogni pretesa o azione che dovesse essere rivolta all'Organizzazione medesima da qualunque soggetto terzo, in conseguenza di tale uso improprio. L'utente non può utilizzare il servizio in modo da pregiudicarne la fruizione da parte degli altri utenti.

Attivazione, Modifica, Revoca, Sospensione e Cancellazione

L'attivazione deve essere richiesta dal Responsabile di Funzione al quale l'Autorizzato deve fare riferimento. Le credenziali di accesso alle singole caselle di posta elettronica dell'istituto saranno dunque nella disponibilità sia dei singoli soggetti autorizzati, che del Titolare del trattamento dati effettuato attraverso lo strumento di posta elettronica dell'istituto. I soggetti autorizzati dovranno adoperare la massima diligenza nel custodire detti codici di accesso e non potranno modificarli, se non previa autorizzazione da parte del Titolare del trattamento.

Per la modifica del servizio di posta elettronica valgono le stesse regole relative all'attivazione del servizio stesso.

Revoca

La casella di posta elettronica verrà disattivata dopo 6 (sei) mesi dalla cessazione del rapporto di lavoro o del rapporto di collaborazione.

Sospensione

L'utilizzo della casella di posta può essere sospeso temporaneamente in caso di violazione della normativa vigente, del presente regolamento, per giustificate motivazioni tecniche o di sicurezza o per sospensione cautelare del dipendente dal servizio.

In quest'ultimo caso il dipendente dovrà fornire alla Istituto un indirizzo alternativo cui potranno essere inviate eventuali comunicazioni utili da parte della Istituto stessa.

Cancellazione

Il contenuto di tutte le caselle postali viene cancellato dopo 12 (dodici) mesi dalla revoca delle caselle stesse.

Firma in calce al messaggio

Il personale autorizzato è tenuto ad apporre ai messaggi di posta elettronica una firma in calce formata da: nome, cognome, struttura d'appartenenza, numeri di telefono, indirizzo sede fisica, evitando di aggiungere altre informazioni non attinenti all'incarico lavorativo.

La Istituto ha la facoltà di inserire in calce a tutte le mail un messaggio o un avviso.

Trattamento Dei Dati Della Casella Di Posta Nominativa In Assenza Dell'utente

L'utente (autorizzato, collaboratore o dipendente) in caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede) - di almeno 5 giornate lavorative - deve attivare l'apposita funzionalità di sistema (cd. "Fuori Sede") che consente di inviare automaticamente ai mittenti un messaggio di risposta contenente le "coordinate" (anche elettroniche o telefoniche) di un altro utente o altre modalità utili di contatto della struttura.

L'Organizzazione, in caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema, si riserva, per mezzo dell'Amministratore di Sistema e Responsabile sistemi, di accedere alla casella di posta elettronica dell'utente assente e/o di modificarne la modalità di consegna e consultazione al fine di garantire la continuità operativa delle funzioni assegnate all'addetto.

Cessazione Del Rapporto Di Lavoro O Collaborazione

Prima della cessazione di ogni tipologia di rapporto con l'Organizzazione, è fatto obbligo all'utente di trasmettere al Responsabile del reparto/ufficio di appartenenza i messaggi di posta elettronica rilevanti

Ministero dell'Istruzione, dell'Università e della Ricerca Ufficio Scolastico Regionale per la Sicilia

C.P.I.A. CT1 CATANIA

Centro Provinciale per l'Istruzione degli Adulti

Via Velletri, 28 – 95126 CATANIA

Cod.Fisc. 93203370874 - Cod.Mecc. CTMM150008

Tel 0958259050 -

e-mail: ctmm150008@istruzione.it pec.: ctmm150008@pec.istruzione.it

per il prosieguo dell'attività istituzionale.

Accesso Ai Dati Dell'utente

L'Amministratore di Sistema può accedere ai dati trattati dall'utente tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware). Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale autorizzato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale autorizzato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni.

Lo stesso Amministratore di Sistema può, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico dell'istituto (ad es. rimozione di file o applicazioni pericolosi).

L'Amministratore di Sistema, in caso di assenza improvvisa o prolungata dell'utente o comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema, è abilitato ad accedere alla posta elettronica dell'utente per le strette necessità operative. Di tale avvenuto accesso dovrà comunque essere data tempestiva comunicazione all'utente.

L'Amministratore di Sistema può procedere a controlli sulla navigazione finalizzati a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.

L'eventuale controllo sui file di log da parte dell'Amministratore di Sistema non è comunque continuativo ed è limitato ad alcune informazioni (es. Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto - Navigazione internet : il nome dell'utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'organizzazione, e comunque non oltre 12 mesi, fatti salvi in ogni caso specifici obblighi di legge.

Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovra registrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico.

L'Amministratore di Sistema è altresì abilitato ed autorizzato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'organizzazione per cessazione del rapporto, sostituzione delle apparecchiature, etc.

Sarà cura dell'utente la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti.

Regole generali

- identificazione dell'interessato:

in alcuni casi, per soddisfare esigenze di verifica dell'identità della persona e garanzia di correttezza del dato da raccogliere, può essere necessario identificare il soggetto interessato ed è, pertanto, opportuno richiedere un documento di identità o di riconoscimento;

- controllo dell'esattezza del dato:

fare attenzione alla digitazione ed all'inserimento dei dati identificativi e personali degli interessati facendo il possibile per evitare errori di battitura che potrebbero creare problemi nella gestione dell'anagrafica e nel prosieguo del processo;

- obbligo di riservatezza e segretezza:

l'Autorizzato al trattamento ha l'obbligo della riservatezza e del segreto sulle informazioni delle quali venga a conoscenza nel corso delle operazioni di trattamento; deve evitare la comunicazione o la diffusione delle informazioni a soggetti non autorizzati o che non abbiano necessità di conoscere i dati trattati. Si ricorda che l'eventuale violazione degli obblighi ivi considerati può comportare l'applicazione di sanzioni di natura disciplinare e configura una responsabilità civile e penale secondo quanto previsto dal Codice della privacy e dal Nuovo Regolamento Europeo;

- tenuta cartelle e fascicoli:

qualora si ricevano nella propria stanza soggetti terzi e si tengano sulla propria scrivania cartelle e fascicoli, si consiglia di fare attenzione a rivoltare le cartelle o di inserire (a seconda delle necessità operative e organizzative) sul frontespizio delle stesse, dati ed informazioni che non permettano a terzi estranei di percepire l'identità dei soggetti interessati dal trattamento;

- distruzione delle copie cartacee:

è necessario prima di gettare la documentazione nel cestino della carta provvedere a renderne non comprensibile il contenuto. Al fine di realizzare il predetto scopo potranno essere utilizzati apparati distruggi documenti o altri più banali accorgimenti come ad esempio lo strappo dei documenti, la separazione del dato identificativo dal resto delle informazioni mediante separazione fisica dei fogli, etc;

CONTROLLI *DA PARTE DELLA* TITOLARITA'

Con il presente capitolo si porta all'attenzione degli Autorizzati la possibilità che questa Istituto effettui controlli sulle proprie apparecchiature tecnologiche al fine di preservare la sicurezza informatica dei dati personali in esse contenuti; rispetto a tali controlli il presente Regolamento costituisce preventiva e completa informazione nei confronti dei dipendenti.

Si sottolinea che la strumentazione tecnologica/informatica e quanto con essa creato è di proprietà della Istituto in quanto mezzo di lavoro. È pertanto fatto divieto di utilizzo del mezzo tecnologico/informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non strettamente coincidenti con quelli della Istituto stessa.

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno

Ministero dell'Istruzione, dell'Università e della Ricerca Ufficio Scolastico Regionale per la Sicilia

C.P.I.A. CT1 CATANIA

Centro Provinciale per l'Istruzione degli Adulti

Via Velletri, 28 – 95126 CATANIA

Cod.Fisc. 93203370874 - Cod.Mecc. CTMM150008

Tel 0958259050 -

e-mail: ctmm150008@istruzione.it pec.: ctmm150008@pec.istruzione.it

realizzati dalla Istituto nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e del presente Regolamento.

In caso di anomalie, la Istituto, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia. In tali casi, il controllo si concluderà con un avviso al Responsabile del reparto/ufficio interessato in cui è stato rilevato l'utilizzo anomalo degli strumenti dell'istituto affinché lo stesso inviti le strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, la Istituto si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite. In nessun caso verranno realizzate verifiche prolungate, costanti o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi della Istituto.

L'Autorizzato, al fine di non esporre sé stesso e la Istituto a rischi sanzionatori, è tenuto ad adottare comportamenti puntualmente conformi alla normativa vigente ed alla regolamentazione dell'istituto. Gli utenti sono responsabili del corretto utilizzo dei servizi di Internet e Posta Elettronica. Pertanto sono responsabili per i danni cagionati al patrimonio, alla reputazione del titolare. Tutti gli utenti sono pertanto tenuti ad osservare e a far osservare le disposizioni contenute nel presente Regolamento il cui mancato rispetto o la cui violazione, costituendo inadempimento contrattuale potrà comportare:

- per il personale dipendente, oltre che l'adozione di provvedimenti di natura disciplinare previsti dal Contratto Collettivo Nazionale di Lavoro vigente, le azioni civili e penali stabilite dalle leggi vigenti;
- per i collaboratori esterni, oltre alla risoluzione del contratto, le azioni civili e penali stabilite dalle leggi vigenti.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Titolare.

Il presente Regolamento è soggetto a revisione con frequenza periodica. Copia del presente Regolamento è consegnata o comunque resa nota a ciascun dipendente all'atto dell'assunzione ed a ciascun collaboratore esterno ad inizio attività.

Catania, 9/10/2019

Il Dirigente Scolastico
(Prof.ssa Antonietta Panarello)
firma autografa sostituita a mezzo stampa ex art. 3 comma 2 D.lgs. 39/93