ISTITUTO OMNICOMPRENSIVO *"Dante Alighieri"*
Via Septempedana, s.n.c. - *06025 NOCERA UMBRA (PG)*
Tel. 0742/818860 - 0742/818701
e-mail: pgic82800p@istruzione.it - pec: pgic82800p@pec.istruzione.it
www.scuolenoceraumbra.edu.it - C.F. 83004080541

Regolamento per l'utilizzo della strumentazione informatica aziendale, della rete internet e delle relative piattaforme utilizzate on site e in cloud

SEDE	**ISTITUTO OMNICOMPRENSIVO "Dante Alighieri"** **Sede Segreteria amministrativa** **Via Septempedana, s.n.c. - 06025 NOCERA UMBRA (PG)**

REV.	DESCRIZIONE REVISIONE	REDATTO DA	VERIFICATO DA	AUTORIZZATO PER L'EMISSIONE	DATA
00	Prima emissione				06/04/2018
01	Revisione				14/05/2019
02	Revisione				10/01/2022

Sommario

OGGETTO E FINALITÀ

Il presente Regolamento è redatto:

- alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- in attuazione del Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR);
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa».

La finalità è quella di promuovere in tutto il personale docente una corretta "cultura informatica" affinché l'utilizzo degli Strumenti informatici e telematici forniti dall'Organizzazione sia conforme alle finalità per le quali sono state messe a disposizione del personale e nel pieno rispetto della legge. Si vuole fornire a tutto il personale le indicazioni necessarie con l'obiettivo primario di evitare il verificarsi di qualsiasi abuso o uso non conforme, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

SEZIONE I - I PRINCIPI

Art. 1 - Introduzione, definizioni e finalità

Il presente disciplinare interno ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo l'utilizzo della strumentazione informatica aziendale, della rete internet e delle relative piattaforme utilizzate da parte degli utenti assegnatari (docenti, dipendenti, collaboratori ecc.), al fine di tutelare i beni dell'Organizzazione ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre l'ISTITUTO OMNICOMPRENSIVO "Dante Alighieri" (d'ora in avanti "Organizzazione") a problematiche di sicurezza, di immagine, risorse e patrimoni per eventuali danni, cagionati anche a terzi.

L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare l'Organizzazione ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano.

A tal fine, pertanto, si rileva che gli eventuali controlli ivi previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa di cui sopra.

Art. 2 - Ambito di applicazione

Il presente disciplinare interno si applica ad ogni Utente assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informative di pertinenza dell'Organizzazione.

Per Utente si intende, pertanto, a titolo esemplificativo e non esaustivo, ogni docente, dipendente, collaboratore (interno o esterno), consulente, fornitore e/o terzo che in modo continuativo e non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici. Per Organizzazione si intende, invece, l'Istituzione, l'Azienda, l'Organizzazione e/o comunque il Titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

Art. 3 - Titolarità dei beni e delle risorse informatiche

I beni e le risorse informatiche, i servizi ICT e le reti informatiche costituiscono beni dell'Organizzazione rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà dell'Organizzazione stessa. Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative affidate ad ogni Utente in base al rapporto in essere (ovvero per scopi professionali afferenti all'attività svolta per l'Organizzazione), e comunque per l'esclusivo perseguimento degli obiettivi dell'Organizzazione.

A tal fine si precisa sin d'ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'Organizzazione, sarà dallo stesso considerato come avente natura dell'Organizzazione e non riservata.

Art. 4 - Responsabilità personale dell'utente

Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'Organizzazione nonché dei relativi dati trattati per finalità perseguite dall'Organizzazione stessa. A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con L'Organizzazione, è tenuto a tutelare (per quanto di propria competenza) il patrimonio informativo da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia.

L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse interne. Ogni Utente, pertanto, è tenuto, in relazione al proprio ruolo e alle mansioni in concreto svolte, ad operare a tutela della sicurezza informatica, riportando al proprio responsabile e senza ritardo, eventuali rischi di cui è a conoscenza ovvero violazioni del presente disciplinare interno. Sono vietati comportamenti che possano creare un danno, anche di immagine, all'Organizzazione.

Art. 5 - I controlli

- I principi

Controlli sui dispositivi/postazioni informatiche (art. 6.1 Provv. Garante [Doc-Web: 1387522], ad integrazione dell'Informativa ex art. 13 GDPR) .

Poiché in caso di violazioni contrattuali e giuridiche, sia il datore di lavoro, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Organizzazione verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2) e s.m.i., di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori.

Nell'effettuare controlli sull'uso degli strumenti elettronici l'Organizzazione dichiara di evitare ogni interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata sottolineando che eventuali sistemi atti a monitorare presumibili violazioni di legge o comportamenti anomali da parte degli Utenti avvengono nel rispetto con esclusione di registrazioni o verifiche con modalità sistematiche e secondo i principi seguenti:

- **Proporzionalità**: il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
- **Trasparenza**: l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.

- **Pertinenza e non eccedenza**: ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

L'Organizzazione, nel riservarsi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici interni (artt. 2086, 2087 e 2104 c.c.), agirà in base al principio della "**gradualità**".

Secondo questo principio:

- I controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura interna ovvero a singole aree lavorative.
- Nel caso in cui si dovessero riscontrare violazioni del presente disciplinare interno, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà diffuso un avviso generalizzato, o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici utilizzati, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite.
- In caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

- I controlli non autorizzati

In ogni caso l'Organizzazione non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore. Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- la memorizzazione sistematica delle pagine internet visualizzate da ciascun Utente, dei contenuti ivi presenti e del tempo di permanenza sulle stesse;
- la lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;
- l'analisi dei dispositivi per l'accesso alla rete internet.

SEZIONE II - MISURE ORGANIZZATIVE

Art. 6 - Amministratori del sistema[1]

(rif. principi di "Accountability", "Privacy by design" e "Privacy by default" Reg.UE 679/2016)

Nel nuovo Regolamento europeo sulla protezione dei dati personali (GDPR) non c'è un chiaro riferimento alla figura dell'amministratore di sistema nel processo di trattazione e custodia dei dati, pur trattandosi di una figura implicitamente richiamata, in alcune norme[1], per le sue specifiche competenze tecniche.

L'Organizzazione, nel caso ritenga di nominare uno o più amministratori di sistema, conferisce all'amministratore stesso ovvero al Titolare del Trattamento, il compito di sovrintendere i beni e le risorse informatiche interne.

Sarà compito della figura preposta:

1) gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'Organizzazione;
2) gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;

[1] Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) (così modificato in base al provvedimento del Garante Privacy del 25 giugno 2009)

3) monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
4) creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
5) rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
6) provvedere alla sicurezza informatica dei sistemi informativi, nel rispetto del principio di "Accountability" del Reg. UE 2016/679;
7) utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un Utente in caso di prolungata assenza, irrintracciabilità o impedimento dello stesso. Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di Privacy Officer[2] all'interno dell'Organizzazione e della "Funzione Privacy" e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

Art. 7 - Assegnazione degli account e gestione delle password

- Creazione e gestione degli Account

Un account Utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche dell'Istituzione scolastica, per singola postazione lavorativa.

- Gli account utenti vengono creati dagli amministratori di sistema e/o gestore dei sistemi e/o rappresentante del Titolare del Trattamento e sono personali, ovvero associati univocamente alla persona assegnataria.
- L'accesso ai propri account scolastici (distinti per servizio assegnato con la formula SaaS[3]) avviene tramite l'utilizzo delle "credenziali di autenticazione" (es. "Username" e "Password"), comunicate all'Utente dagli amministratori di sistema e/o gestori dei sistemi e/o rappresentanti del Titolare del Trattamento, vengono generate attraverso modalità che ne garantiscano la segretezza (es: busta chiusa e sigillata e/o comunicazione elettronica crittografata).
- Le credenziali di autenticazione fanno parte dei dati della scuola da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi (seppur soggetti in posizione apicale all'interno dell'Organizzazione).
- Se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password e/o a segnalare la violazione agli amministratori di sistema e/o gestore dei sistemi e/o rappresentante del Titolare del Trattamento nonché al Responsabile privacy di riferimento.
- Ogni Utente è responsabile dell'utilizzo del proprio account Utente.
- Si ricorda che in caso di assenza improvvisa o prolungata del lavoratore/docente e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive della scuola o per la sicurezza ed operatività delle risorse informatiche dell'Organizzazione, lo stesso si riserva

[2] Il privacy officer (in inglese, "agente della privacy") è una figura professionale con competenze giuridiche, informatiche e gestionali, la cui responsabilità principale è osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'organizzazione, affinché questi siano trattatati in modo lecito e pertinente, nel rispetto delle normative vigenti.

[3] Software-as-a-Service (SaaS) è un servizio di cloud computing che offre agli utenti finali un'applicazione cloud, munita di piattaforme e dell'infrastruttura IT che la supportano, tramite un browser web

la facoltà di accedere a qualsiasi dotazione e/o apparato assegnato in uso all'Utente per mezzo dell'intervento dagli amministratori di sistema e/o gestore dei sistemi e/o rappresentante del Titolare del Trattamento.

- Si ricorda, infine, che i beni e la strumentazione informatica oggetto del presente disciplinare interno rimane di esclusivo dominio dell'Organizzazione, il quale, in virtù dei rapporti instaurati con gli utenti, ne disciplina l'affidamento.

- Gestione e utilizzo delle password

Dopo la prima comunicazione delle credenziali di autenticazione, l'Utente ha il compito di modificare, al suo primo utilizzo, la propria password, procedendo allo stesso modo ogni 6 mesi (nel caso di trattamento di dati particolari sensibili e giudiziari la parola chiave è modificata almeno ogni 3 mesi).

L'Utente, nel definire il valore della password, deve rispettare le seguenti regole:

- utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, @, ecc.), di cui almeno uno numerico;
- la password deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "@#§f$' ... ";
- evitare di includere parti del nome, cognome e/o comunque elementi a lui agevolmente riconducibili;
- evitare l'utilizzo di password comuni e/o prevedibili;
- proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi. Si ricorda che scrivere la password su post-it o altri supporti non è conforme alla normativa e costituisce violazione del presente disciplinare interno.

- Cessazione degli Account

In caso di interruzione del rapporto di lavoro con l'Utente, le credenziali di autenticazione di cui sopra verranno disabilitate entro un periodo massimo di 30 giorni da quella data; entro 6 mesi, invece, si disporrà la definitiva e totale cancellazione dell'account Utente.

Art. 8 - Postazioni di lavoro

Per postazione di lavoro si intende il complesso unitario di Personal Computer (di seguito, PC), notebook, tablet, Ipad, Chromebook, accessori, periferiche e ogni altro device concesso dall'Organizzazione in utilizzo all'Utente. L'assegnatario di tali beni e strumenti informatici dell'organizzazione, pertanto, ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile. Al fine di disciplinare un corretto utilizzo di tali beni, l'Organizzazione ha adottato le regole tecniche, che di seguito si riportano:

- Ogni PC, notebook (accessori e periferiche incluse), e altri devices, sia esso acquistato, noleggiato, o affidato in locazione, rimane di esclusiva proprietà dell'Organizzazione, ed è concesso all'Utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti all'attività svolta.
- È dovere di ogni Utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente.
- Il PC e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dall'Organizzazione. Per utilizzare software o applicativi non presenti nella dotazione standard fornita, si necessita di espressa richiesta scritta dell'utente indirizzata al proprio Privacy Officer[4] di riferimento, amministratore di sistema e/o gestore dei sistemi e/o rappresentante del Titolare del Trattamento, il quale ne valuterà i requisiti tecnici e l'aderenza alle policy interne ed al ruolo ricoperto in Organizzazione.

[4] Il privacy officer (in inglese, "agente della privacy") è una figura professionale con competenze giuridiche, informatiche e gestionali, la cui responsabilità principale è osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'organizzazione, affinché questi siano trattatati in modo lecito e pertinente, nel rispetto delle normative vigenti.

- Le postazioni di lavoro non devono essere lasciate incustodite con le sessioni utenti attive.
- Quando un Utente si allontana dalla propria postazione di lavoro, deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione.
- L'Utente deve segnalare con la massima tempestività all'amministratore di sistema e/o gestore dei sistemi e/o rappresentante del Titolare del Trattamento, eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature.
- È fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici dell'Istituzione scolastica a soggetti terzi.
- L'Organizzazione si riserva la facoltà di rimuovere qualsiasi elemento hardware la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.

Device di proprietà personale dell'Utente quali computer portatili, telefoni cellulari, tablet, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, ecc. **non potranno essere collegati ai computer o alle reti informatiche della scuola, salvo preventiva autorizzazione scritta dell'Organizzazione stessa e conseguente configurazione secretata dell'Amministratore di sistema**.

SEZIONE III - CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 9 - Personal computer, computer portatili ed altre devices

Gli utenti utilizzano, per l'espletamento delle proprie mansioni, dispositivi e software di proprietà (o, comunque, gestite dall'Organizzazione) e/o di device personali preventivamente approvati e configurati dalla scuola insieme con piattaforme in cloud per lo svolgimento dei propri compiti e in funzione della didattica.

Nella fattispecie: Registro Elettronico e Google Workspace for Education (Gmail, Calendar, Classroom, Drive, Documenti, Moduli, Fogli, Presentazioni, Talks/Hangouts, Meet, servizi aggiuntivi es. Youtube, Blogger).

Ne consegue che gli stessi utenti sono tenuti al rispetto delle seguenti regole:

- Non è consentito modificare la configurazione hardware e software del proprio device, se non previa esplicita autorizzazione dell'Organizzazione che la esegue per mezzo dell'amministratore di sistema e/o gestore dei sistemi e/o rappresentante del Titolare del Trattamento.
- Non è consentito rimuovere, danneggiare o asportare componenti hardware.
- Non è consentito installare autonomamente programmi informatici, software ed ogni altro applicativo non autorizzato espressamente dall'Organizzazione.
- È onere dell'Utente, in relazione alle sue competenze, eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus nonché sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore di sistema e/o gestore dei sistemi e/o rappresentante del Titolare del Trattamento.
- È onere dell'Utente spegnere il proprio PC, computer portatile, tablet al termine del lavoro.

Per quanto concerne, invece, la gestione dei computer portatili, tablet e/o altri devices non fisse l'Utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali files elaborati prima della sua riconsegna.

Non è consentito all'Utente caricare o inserire all'interno del portatile/tablet e/o altri devices non fisse qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli utenti di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile/tablet e/o altri devices non fissi agli uffici competenti per la restituzione o la riparazione.

Art. 10 - Software

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno ottenere espressa autorizzazione dell'Organizzazione per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria ("freeware" o "shareware").

L'Organizzazione richiama l'attenzione del proprio personale su alcuni aspetti fondamentali che l'Utente è tenuto ad osservare per un corretto utilizzo del software on site ed in cloud dell'Organizzazione:

- L'Organizzazione acquista/noleggia/gestisce le licenze d'uso dei software on site e servizi on line specifici per la scuola da vari fornitori esterni. L'Utente, pertanto, è soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei contratti di licenza e di prescrizioni di utilizzo scolastico.
- Non è consentito fare né il download né l'upload tramite internet di software non autorizzato.
- L'Organizzazione, sulla scorta di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione.
- L'Organizzazione non tollererà la duplicazione/utilizzo illegale del software.

Art. 11 - Dispositivi di memoria portatili

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, files, o documenti esternamente al computer.

Sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, riproduttori musicali MP3, fotocamere digitali, dischi rigidi esterni, ecc. L'utilizzo di tali supporti risponde alle direttive che di seguito si riportano:

- non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dall'Organizzazione;
- è onere dell'Utente custodire i supporti magnetici contenenti dati particolari (ex sensibili) e giudiziari in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto;
- si precisa che, ove autorizzati in base a quanto sopra disposto, una volta connessi all'infrastruttura informatica dell'Organizzazione, i dispositivi saranno soggetti (ove compatibili) al presente disciplinare interno.

Art. 12 - Stampanti, fotocopiatrici e fax

L'utilizzo dei suddetti strumenti deve avvenire sempre per scopi istituzionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte dell'Organizzazione.

È richiesta una particolare attenzione quando si inviano documenti su una stampante condivisa aventi ad oggetto dati personali o informazioni riservate; ciò al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa.

L'utilizzo dei fax per l'invio di documenti che hanno natura strettamente confidenziale, è generalmente da evitare. Nei casi in cui questo sia necessario, si deve preventivamente avvisare il destinatario, in modo da ridurre il rischio che persone non autorizzate possano venirne a conoscenza, e successivamente chiedere la conferma telefonica di avvenuta ricezione.

SEZIONE IV - GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 13 - Gestione utilizzo della rete internet

Ogni Utente potrà essere abilitato, dall'Organizzazione, alla navigazione Internet. Col presente disciplinare interno si richiamano gli utenti ad una particolare attenzione nell'utilizzo di Internet e dei servizi relativi, in quanto ogni operazione posta in essere è associata all' ''Indirizzo Internet Pubblico" assegnato all'Organizzazione stessa. Internet è uno strumento messo a disposizione degli utenti per uso istituzionale.

Ciascun lavoratore, pertanto, deve quindi usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia;

l'Utente deve quindi prendere ogni precauzione a tale riguardo.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet so no le seguenti:

a) L'utilizzo è consentito esclusivamente per scopi istituzionali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative.
b) Non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dall'Organizzazione.
c) È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
d) Non sono permesse, se non per motivi istituzionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in guest-book, anche utilizzando pseudonimi (o nicknames).
e) Non è consentita la navigazione in siti dove potrebbe essere possibile ricevere e inviare informazioni di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
f) È consentito l'utilizzo di soluzioni di Instant Messenger e/o chat esclusivamente per scopi istituzionali ed attraverso gli strumenti ed i software messi a disposizione dall'Organizzazione.
g) Non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo.
h) Non è consentito lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, ecc., protetto da copyright.
i) Non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'Organizzazione in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente;

È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere nocivo all'immagine dell'Organizzazione.

Per facilitare il rispetto delle predette regole, L'Organizzazione si riserva, per mezzo dell'amministratore di sistema, e/o gestore dei sistemi e/o rappresentante del Titolare del Trattamento, la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di file o software).

Art. 14 - Gestione e utilizzo della posta elettronica istituzionale

- ### Principi guida

Ad ogni Utente titolare di un account, L'Organizzazione provvede ad assegnare una casella di posta elettronica individuale (es. mario.rossi@scuolenoceraumbra.it . I servizi di posta elettronica devono essere utilizzati a scopo istituzionale: si ricorda a tutti gli utenti che l'account e-mail è uno strumento di proprietà dell'Organizzazione ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate.

Ad uno stesso Utente possono essere assegnate più caselle di posta elettronica che possono essere condivise con altri utenti dello stesso gruppo/dipartimento. Tali caselle devono essere utilizzate esclusivamente per la ricezione dei messaggi, mentre per le risposte o gli invii, si deve sempre utilizzare la casella di posta assegnata.

L'Organizzazione, valuterà caso per caso e previa richiesta dell'Utente, la possibilità di attribuire allo stesso un diverso indirizzo destinato ad uso privato. Attraverso l'e-mail della scuola, gli utenti rappresentano pubblicamente l'Organizzazione e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da non compromettere, altresì, l'immagine istituzionale (reputazione).

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica della scuola e sono tenuti ad utilizzarle in modo conforme alle presenti regole.

Gli stessi, pertanto, devono:

- conservare la password nella massima riservatezza e con la massima diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
- utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché della posta ricevuta. Gli allegati provenienti da **mittenti sconosciuti** non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (es. virus);
- inviare preferibilmente files in formato PDF;
- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i files attachment di posta elettronica prima del loro utilizzo;
- rispondere ad e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
- collegarsi a siti internet contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto degli stessi.

Non è consentito agli utenti, al contrario:

- diffondere il proprio indirizzo e-mail istituzionale attraverso la rete internet;
- non utilizzare la casella di posta elettronica affidata per inviare, ricevere o scaricare allegati contenenti video, brani musicali, ecc., salvo che questo non sia funzionale all'attività prestata in favore dell'Organizzazione (es.: presentazioni o materiali video per l'attività scolastica).

Si ricorda che, salvo l'utilizzo di appositi strumenti di cifratura**, i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse**. Pertanto, si richiede agli utenti di valutare con attenzione l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale".

Occorre inoltre che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

- ### Accesso alla casella di posta elettronica del lavoratore assente

Saranno messe a disposizione di ciascun Utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che consentano di inviare automaticamente, in caso di assenze

programmate, messaggi di risposta che contengano le coordinate di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza del lavoratore.

- In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail dell'Organizzazione), perdurando l'assenza oltre un determinato limite temporale pari a 30 giorni, disporrà lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l'amministratore di sistema oppure, se presente, un incaricato interno per la protezione dei dati e/o comunque il Titolare del trattamento), l'attivazione di un analogo accorgimento (risposta automatica o re-indirizzamento), avvertendo l'assente.

Nel caso, invece, L'Organizzazione necessiti conoscere il contenuto dei messaggi di posta elettronica dell'Utente resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:

- la verifica del contenuto dei messaggi sarà effettuata per il tramite di idoneo "fiduciario", da intendersi quale lavoratore previamente nominato e/o incaricato (per iscritto) dall'Utente assente;
- di tale attività sarà redatto apposito verbale e informato l'Utente interessato alla prima occasione utile.

- Cessazione dell'indirizzo di posta elettronica istituzionale

In caso di interruzione del rapporto di lavoro con l'Utente, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 giorni da quella data; entro 6 mesi, invece, si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'Organizzazione si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti.

Art. 15 - Sanzioni

L'eventuale violazione di quanto previsto dal presente disciplinare interno - rilevante anche ai sensi degli artt. 2104 e 2105 c.c. - potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 dello Statuto dei Lavoratori.

L'Organizzazione avrà cura di informare senza ritardo (e senza necessità di preventive contestazioni e/o addebiti formali) le autorità competenti, nel caso venga commesso un reato, o la cui commissione sia ritenuta probabile o solo sospettata, tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici istituzionali.

Si precisa, infine, che in caso di violazione accertata da parte degli utenti delle regole e degli obblighi esposti in questo disciplinare, L'Organizzazione si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici.

Art. 16 - Informativa agli utenti ex art. 13 Regolamento UE n. 2016/679

Il presente disciplinare interno, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informativi della scuola, e relativamente ai trattamenti di dati personali svolti dall'Organizzazione e finalizzati alla effettuazione di controlli leciti, così come definiti nell'art. 5, vale quale informativa ex art. 13 del Regolamento UE n. 2016/679.

Art. 17 - Comunicazioni

Il presente disciplinare interno è messo a disposizione degli utenti, per la consultazione, al momento dell'assegnazione di un account Utente. Sulla intranet istituzionale, ovvero presso la bacheca della scuola è pubblicata la versione più aggiornata dello stesso allo scopo di facilitarne la conoscibilità a tutti gli interessati.

Ad ogni aggiornamento del presente documento, ne sarà data comunicazione sulle bacheche istituzionali e tramite l'invio di apposito messaggio e-mail.

Tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata del presente disciplinare. Le autorizzazioni e/o concessioni richieste in base al presente disciplinare ovvero poste nella facoltà degli utenti potranno essere comunicate all'Organizzazione per mezzo di qualsiasi strumento che ne garantisca la tracciabilità (es.: e-mail).

Art. 18 - Approvazione del presente regolamento disciplinare

Il presente disciplinare interno, è stato approvato dal Collegio docenti dell'Organizzazione in data 28/10/2022 e del Commissario Straordinario in data 31/10/2022 e sono stati oggetto di condivisione con le rappresentanze sindacali della scuola, in ottemperanza a quanto previsto dall'art. 4 della legge n. 300/1970 (Statuto dei Lavoratori).

Il Titolare del trattamento, nella persona del legale rappresentante

Prof. Leano Garofoletti

_____