

**ISTITUTO COMPRENSIVO  
“V.TORTORETO”**

**Via Roma, 35 62026 - San Ginesio (MC)**

**C.F. 83004250433**

**Mail: [mcic80600@istruzione.it](mailto:mcic80600@istruzione.it)  
PEC: [mcic8060@pec.istruzione.it](mailto:mcic8060@pec.istruzione.it)**

**REGOLE SULL'UTILIZZO DEGLI STRUMENTI  
INFORMATICI, DI INTERNET E DELLA POSTA  
ELETTRONICA**

NR Rev	Descrizione modifiche	Data
0	Prima stesura	Marzo 2019

## **Indice**

### **Premessa**

1. Entrata in vigore del regolamento e pubblicità
2. Campo di applicazione del regolamento
3. Utilizzo delle stazioni di lavoro
4. Gestione ed assegnazione delle credenziali di autenticazione
5. Utilizzo della rete
6. Utilizzo e conservazione dei supporti rimovibili
7. Uso della posta elettronica
8. Navigazione in Internet
9. Protezione antivirus
10. Utilizzo dei telefoni
11. Accesso ai dati trattati dall'utente
12. Sanzioni
13. Norme finali
14. Aggiornamento e revisione

## **Premessa**

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone la Società e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, **l'Istituto Comprensivo** ha adottato un Regolamento interno diretto ad evitare anche comportamenti inconsapevoli che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Ogni utilizzo delle apparecchiature, degli elaboratori, delle reti e dei dati diversi dalle finalità professionali deve essere strettamente limitato e di natura occasionale, salve le eccezioni espressamente previste nel presente Regolamento. Poiché anche nella normale attività lavorativa, alcuni comportamenti possono mettere a rischio la Sicurezza e l'immagine dell'istituto, di seguito vengono richiamate semplici regole procedurali finalizzate non tanto a censurare comportamenti consapevolmente scorretti e già di per sé proibiti, ma soprattutto per evitare condotte che inconsapevolmente possano causare rischi alla Sicurezza del trattamento dei dati aziendali.

A seguito dell'emanazione, da parte del Garante per la Protezione dei Dati Personali, del provvedimento generale del 1 marzo 2007 avente ad oggetto "Linee guida del Garante per posta elettronica e internet" ed al fine di conciliare l'esigenza di tutela della privacy dei dipendenti e collaboratori ed il corrispondente potere/dovere del Titolare di assicurare la funzionalità e il corretto impiego degli strumenti informatici da parte degli stessi, l'Istituto Comprensivo ha adottato il presente

**Disciplinare interno** che regola, pur nel rispetto dei principi di pertinenza e non eccedenza, le modalità di utilizzo da parte dei suddetti dipendenti e collaboratori della rete ed in genere di tutti gli strumenti tecnologici aziendali.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Regolamento UE n. 2016/679 contenente le misure minime di

sicurezza, nonché integrano le informazioni già fornite agli interessati in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

### **1. Entrata in vigore del regolamento e pubblicità**

Il nuovo regolamento entrerà in vigore il [●], salvo successive modifiche ed integrazioni. Con l'entrata in vigore del presente regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

Copia del regolamento oltre ad essere affisso negli uffici dell'amministrazione potrà essere fornito a tutti i dipendenti.

### **2. Campo di applicazione del regolamento**

Il nuovo regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori della scuola a prescindere dal rapporto contrattuale con la stessa intrattenuto.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

Allo scopo di consentire a questi strumenti di perseguire le finalità per le quali sono stati acquisiti, e al fine di garantire che gli strumenti di lavoro possano mantenere le loro funzionalità senza essere danneggiati, anche a seguito di eventuali comportamenti non corretti degli operatori, si danno qui di seguito alcune informazioni e regole di utilizzo cui tutti, dipendenti e collaboratori, dovranno attenersi.

### **3. Utilizzo delle stazioni di lavoro**

**La stazione di lavoro (pc, terminale o notebook) affidata all'utente è uno strumento di lavoro.** L'Istituto Comprensivo fornisce il necessario supporto agli utenti per il corretto utilizzo delle postazioni di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. La

stazione di lavoro deve essere custodita con cura evitando ogni possibile forma di danneggiamento. Gli utenti sono tenuti a conservare le stazioni di lavoro nella configurazione loro assegnata; è quindi vietato:

- togliere/aggiungere/cambiare componenti hardware e software;
- cambiare l'ubicazione delle apparecchiature, senza la preventiva autorizzazione della l'Istituto Comprensivo.

La configurazione della stazione di lavoro prevede che i dati siano residenti sulle unità di rete a disposizione.

L'utilizzo in rete di PC e di qualsiasi altra attrezzatura informatica personale di dipendenti e di terzi è consentita previa autorizzazione dell'amministrazione, che ne stabilisce le modalità di accesso.

I dati riservati di norma non possono essere registrati su PC portatili; diversamente sono gestiti sotto il controllo dell'Istituto Comprensivo.

La postazione di lavoro data in affidamento all'utente permette l'accesso alla rete dell'Istituto Comprensivo solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 4 del presente Regolamento.

L'Istituto Comprensivo rende noto che il personale operante sui dispositivi aziendali è stato preventivamente autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.). Detti interventi, in considerazione dei divieti di cui ai successivi punti nn. 7 e 8, potranno anche comportare l'accesso in occasione dei controlli necessari ai fini della **corretta manutenzione ed uso degli strumenti** elettronici: ciò consentirà l'eventuale accesso ai dati trattati da ciascuna stazione di lavoro, ivi compresi gli archivi di posta elettronica, nonché i dati relativi alla navigazione nei siti internet acceduti dagli utenti abilitati. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata od impedimento dell'utente.

Il personale incaricato dell'assistenza ICT ha la facoltà, previa autorizzazione dell'Istituto Comprensivo, di collegarsi e visualizzare in remoto il desktop delle singole stazioni di lavoro al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata e/o

autorizzazione dell'utente o, in caso di oggettiva necessità ed urgenza, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone l'Istituto Comprensivo a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

Salvo preventiva espressa autorizzazione dell'Istituto Comprensivo, non è consentito all'utente modificare le caratteristiche impostate sulla propria stazione di lavoro né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc.).

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministrazione nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

La stazione di lavoro deve essere spenta prima di lasciare l'Istituto o in caso di assenze prolungate o in caso di suo perdurante inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso

#### **4. Gestione ed assegnazione delle credenziali di autenticazione**

Le credenziali di autenticazione per l'accesso vengono assegnate dal personale incaricato, previa formale richiesta.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), associato ad **una parola chiave (password) riservata** che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata.

È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del

trattamento, al primo utilizzo e, successivamente, **almeno ogni sei mesi** come previsto dal sistema informativo installato in Azienda. Il sistema avvertirà l'utente della scadenza della password e della necessità di modifica della stessa.

La parola chiave, formata da lettere (maiuscole o minuscole) e numeri e/o caratteri speciali, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, dovrà procedere in tal senso d'intesa con il personale incaricato all'assistenza.

## **5. Utilizzo della rete**

Per l'accesso alla rete ciascun utente deve essere in possesso della specifica credenziale di autenticazione.

È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

Le cartelle utenti 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 in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back-up da parte del personale dell'Istituto. Si ricorda che tutti i dischi o altre unità di memorizzazione locali (es. disco C: interno PC) non sono soggette a salvataggio da parte dell'Istituto Comprensivo. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

Il personale di assistenza, in caso di identificazione di file o applicazioni in genere pericolose per la sicurezza della rete e/o dei singoli PC, potrà procedere alla rimozione degli stessi, previa comunicazione all'utente incaricato.

Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

## **6. Utilizzo e conservazione dei supporti rimovibili**

Tutti i supporti magnetici rimovibili (CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare l'amministrazione e seguire le istruzioni da questo impartite.

In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

Non è consentita l'uscita dalle sedi aziendali di hardware e supporti magnetici, ottici o cartacei, se non preventivamente autorizzati.

E' vietato l'utilizzo di supporti rimovibili personali.

L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

E' interdetta l'installazione o l'uso di supporti rimovibili sulle stazioni di lavoro. Per eventuali necessità in proposito occorrerà farsi autorizzare dall'Istituto Comprensivo.

## **7. Uso della posta elettronica**

Gli utenti, autorizzati a l'utilizzo della p.c., potranno utilizzare nei dispositivi aziendali solo l'account di posta elettronica ufficiale "@istruzione.it" dato dalla P.A. competente. E' fatto espresso ed esplicito divieto di utilizzare qualsiasi altro servizio di posta elettronica non istituzionale.

## **8. Navigazione in Internet**

9.1. La stazione di lavoro assegnata al singolo utente ed abilitata alla navigazione in Internet costituisce uno strumento per lo svolgimento della propria attività lavorativa. È quindi proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo quanto in appresso specificato.

In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:



- l'upload o il download di software gratuiti (freeware e shareware), nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (es.: filmati e musica) e previa verifica dell'attendibilità dei siti in questione.
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat-line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dall'Istituto Comprensivo;

E' tuttavia consentito ai dipendenti di poter accedere per finalità personali a siti di informazione (Giornali e quotidiani) e/o di altro genere (es. siti prenotazione treni/aerei/home banking) purché per un periodo di tempo assai limitato e solo per eventuali necessità ed urgenze. Tale navigazione per finalità personali deve essere comunque improntata a criteri di buona fede e correttezza e non può in alcun caso pregiudicare il disbrigo assiduo e diligente delle mansioni assegnate.

Gli eventuali controlli, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 30 giorni, ossia il tempo indispensabile per il corretto perseguimento delle finalità di sicurezza dell'azienda.

## **9. Protezione antivirus**

Il sistema informatico è protetto da software antivirus aggiornato. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo (evitando, quindi, di compiere quei comportamenti vietati dal presente regolamento e già menzionati: es. navigazione su siti non sicuri, download di file non autorizzati, etc.). E' fatto assoluto divieto a ciascun utente di modificare le impostazioni del software antivirus.

Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso nonché segnalare prontamente l'accaduto al personale di assistenza.

Ogni dispositivo magnetico di provenienza esterna all'Istituto Comprensivo dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus

non dovrà essere utilizzato..

#### **10. Accesso ai dati trattati dall'utente**

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà dell'Istituto Comprensivo, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

#### **11. Sanzioni**

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché con tutte le azioni civili e penali consentite.

#### **12. Norme finali.**

Le disposizioni del presente regolamento si applicano, per quanto compatibili, anche alle ipotesi di collegamento alla rete aziendale da postazioni esterne all'ufficio (ad esempio: collegamento da casa).

#### **13. Aggiornamento e revisione**

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dall'Istituto Comprensivo.

Il presente Regolamento è soggetto a revisione con frequenza annuale.