Ministero dell'Istruzione, dell'Università e della Ricerca
ISTITUTO SCOLASTICO COMPRENSIVO SANT'ELPIDIO A MARE
INFANZIA, PRIMARIA e SECONDARIA DI PRIMO GRADO - C.F. 90055110440 - C.M. APIC839002
Via Carlo Alberto dalla Chiesa n. 114 – 63811 – Sant'Elpidio a Mare (FM)
Tel. 0734.859226/0734.810800 - Fax 0734.818609 – email: apic839002@istruzione.it – web: www.iscsem.gov.it

Prot. 6270/I.1 del 01/12/2018

ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI - RETI DIDATTICHE SENZA SERVER

INDICE

PREMESSA

L'utilizzo delle risorse informatiche e telematiche del nostro Istituto deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro o in un ambiente scolastico.

1- UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer utilizzato dal docente, dallo studente o da altro personale autorizzato è uno **strumento di lavoro e didattico**. Ogni utilizzo non inerente all'attività lavorativa / didattica può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

a. In caso di utilizzo dell'elaboratore privo di account e password, o con account condiviso tra più utenti, è assolutamente vietato salvare documenti contenenti dati personali (o sensibili) nelle cartelle del PC. In caso di accesso autenticato, le credenziali devono essere custodite con la massima diligenza e non divulgate. E' assolutamente vietato lasciare post-it con le password sulla postazione di lavoro.
b. Non è consentito installare autonomamente programmi provenienti dall'esterno senza autorizzazione esplicita del *Personale incaricato alla manutenzione informatica*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
c. Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Personale incaricato alla manutenzione informatica*. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità

con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione 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.

d. Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Personale incaricato alla manutenzione informatica.*
e. Non è consentito far utilizzare la postazione di lavoro a personale non autorizzato
f. Non è consentita l'installazione sul proprio PC di alcun dispositivo esterno,
g. Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Personale incaricato alla manutenzione informatica aziendali* nel caso in cui vengano rilevati virus.

2- UTILIZZO DELLA RETE

a. Il *Personale incaricato alla manutenzione informatica* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
b. Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
c. È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni.

3- GESTIONE DELLE PASSWORD DEI PC / DISPOSITIVI DI RETE

a. È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi
b. Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
c. La password deve essere immediatamente sostituita, dandone comunicazione al *Personale incaricato alla manutenzione informatica aziendali*, nel caso si sospetti che la stessa abbia perso la segretezza.
d. Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al *Personale incaricato alla manutenzione informatica*

4- UTILIZZO DELLE CHIAVETTE USB / HARD DISK ESTERNI

a. L'uso è consentito solo per materiale didattico privo di dati personali (o sensibili), avendo cura preventivamente di rimuovere eventuali virus tramite una scansione.
b. In casi particolari, valutati ed autorizzati dal Dirigente Scolastico, le chiavette usb / hard disk esterni possono essere utilizzati per archiviare dati personali (o sensibili) in modalità criptata specificandone per iscritto il contenuto e le finalità.
c. L'eventuale perdita di tali dispositivi contenenti dati personali / sensibili non criptato costituisce una violazione di sicurezza (DATA BREACH) che deve essere immediatamente comunicata al Dirigente che valuterà se ci sono i presupposti per la notifica all'Autorità di controllo entro 72 ore, secondo le modalità descritte nell' articolo 33 - regolamento UE 2016/679, e la notifica agli interessati senza ingiustificato ritardo (articolo 34 - regolamento UE 2016/679)

5- UTILIZZO DI CARTELLE CLOUD ESTERNE

a. L'uso è consentito solo per materiale didattico privo di dati personali (o sensibili)
b. In casi particolari, valutati ed autorizzati dal Dirigente Scolastico, le cartelle cloud esterne possono contenere dati personali (o sensibili) in modalità criptata specificandone per iscritto il contenuto e le finalità.
c. L'eventuale violazione delle cartelle in cloud, contenenti dati personali / sensibili non criptato costituisce una violazione di sicurezza (DATA BREACH) che deve essere immediatamente comunicata al Dirigente che valuterà se ci sono i presupposti per la notifica all'Autorità di controllo entro 72 ore, secondo le modalità descritte nell' articolo 33 - regolamento UE 2016/679, e la notifica agli interessati senza ingiustificato ritardo (articolo 34 - regolamento UE 2016/679)

6- UTILIZZO DI PC PORTATILI PERSONALI

a. L'uso deve essere autorizzato dal Dirigente, sia se utilizzati come strumento per trattare dati, sia se utilizzati come dispositivi di navigazione in internet. Valgono le stesse regole già descritte per il punto 3

7- USO DELLA POSTA ELETTRONICA

a. La casella di posta personale, assegnata dall'Istituto all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
b. È fatto divieto di utilizzare le caselle di posta elettronica dell'istituto per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
c. È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
d. Ogni comunicazione ufficiale inviata all'esterno è regolamentata dal Manuale di Gestione della SEGRETERIA DIGITALE
e. È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Personale incaricato alla manutenzione informatica*. Non si devono in alcun caso attivare gli allegati di tali messaggi.
f. Prestare attenzione nell'apertura di allegati diversi dal formato PDF. Cestinare tutte le mail contenenti fatture in quanto le stesse sono inviate tramite il canale FatturaPA. Per ogni dubbio sulla veridicità delle altre mail, inoltrare la comunicazione al *Personale incaricato alla manutenzione informatica*

8- USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

a. Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
b. È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Personale incaricato alla manutenzione informatica*.
c. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.
d. È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

e. È vietata 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).

9- OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679.

10-NON OSSERVANZA DELLA NORMATIVA D'ISTITUTO

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento sono perseguibili con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

11-AGGIORNAMENTO E REVISIONE

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

Il presente Regolamento è soggetto a revisione con frequenza annuale.

La Dirigente Scolastica
Prof.ssa Teresa Santagata

Allegato al Prot. 6270/I.1 del 01/12/2018

Firme per presa visione ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI – RETI DIDATTICHE SENZA SERVER