SECURITY POLICY

Le prescrizioni e istruzioni di seguito illustrate sono da intendersi obbligatorie per tutto coloro che prestano servizio o collaborano, in qualsiasi forma, anche autonoma, nella scuola.

La loro inosservanza potrà costituire infrazione disciplinare, inadempimento contrattuale e dare origine alle responsabilità di legge.

Esse non pregiudicano l'adozione di misure codici e protocolli ulteriori, più specifici e più stringenti, in considerazione della tipologia di dati trattati e dei profili di rischio riscontrati in relazione ai medesimi.

Sezione I - Utilizzo della rete e strutture informatiche

Al fine di tutelare la struttura informatica e i dati in essa conservati le seguenti attività, qualora non specificamente autorizzate, sono da ritenersi vietate:

- Utilizzare la rete informatica e telematica per scopi estranei alle mansioni lavorative assegnate o all'attività professionale oggetto dell'incarico o del rapporto di lavoro;
- Scambiare con altri o comunicare ad altri, o comunque rendere disponibili ad altri, dati relativi al proprio account (ad esempio, username e password, o altre credenziali necessarie a garantire l'accesso riservato alla rete o ai programmi);
- Compiere trasferimenti / cessioni di informazioni (software, dati, ecc), documenti posti ad oggetto di diritti di proprietà intellettuale.
- Cancellare, copiare o asportare con qualsiasi mezzo, dati della scuola o programmi software per scopi personali.
- ostacolare l'operatività e l'utilizzabilità della rete, anche da parte di altri utenti.
- Installare, eseguire o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (ad es. virus, *cavalli di Troia*, c.d. *Troy horses*, *spamming*).
- Installare / eseguire programmi software incompatibili con l'attività lavorativa o ad essa estranei così come installare elementi *hardware* incompatibili con l'attività lavorativa.
- Rimuovere, danneggiare o asportare componenti *hardware*.
- Utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività di altri utenti, per leggere, copiare o cancellare files e software di altri utenti.
- Utilizzare *software* volti alla violazione della sicurezza del sistema e della privacy.
- Inserire password locali alle risorse informatiche assegnate (come ad esempio password che rendano inaccessibile il computer agli amministratori di rete).

- memorizzare, “salvare” (su ogni tipo di supporto come “chiavette” USB e dischi removibili), scambiare files relativi al materiale protetto da copyright, di cui non si ha diritto d’uso o per i quali tale diritto è stato concesso per finalità diverse, nonché di materiale pornografico o lesivo della dignità o dei diritti inviolabili delle persone, così come altri eventuali files protetti dalla normativa sul diritto di autore o proprietà intellettuale. Si rammenta che tali attività saranno inoltre perseguite ai sensi di legge, informando le autorità competenti, in caso di illeciti penalmente rilevanti.

Sezione II – Credenziali d’accesso e Amministratore di sistema

Regole generali.

Ad ogni utente / collaboratore è fatto obbligo di:

- mantenere segrete le proprie credenziali di accesso (password e/o pin);
- non lasciare libero accesso ai propri dispositivi in caso di assenza momentanea dalla propria postazione lavorativa;
- controllare l’accesso ad internet ed ai servizi di posta elettronica;
- verificare la presenza di eventuali tracce sospette o insolite prima di utilizzare supporti rimovibili, quali pendrive e memory card:;
- effettuare backup periodici secondo le *best practice* o istruzioni ricevute;

Si ricorda a tal fine che le credenziali di ingresso alla rete e ai programmi, generate ed attribuite inizialmente dall’Amministratore di sistema, dovranno essere modificate al successivo primo accesso nonché successivamente secondo la periodicità i criteri e le esigenze di volta in volta comunicate.

Le password utilizzate dovranno essere generate in modo casuale ed essere formate con un criterio di complessità adeguato, ad esempio: da lettere (maiuscole o minuscole) e numeri; e da almeno otto caratteri; non devono contenere riferimenti agevolmente riconducibili all’incaricato.

Nel caso si sospetti che la propria credenziale di accesso ai sistemi “password” abbia perso il requisito della “segretezza”, si dovrà provvedere alla modificazione immediata della stessa.

Qualora l’utente venga a conoscenza delle password di un altro utente è tenuto a darne immediata notizia all’Amministratore del sistema, affinché provveda alla relativa sostituzione o modificazione.

Procedure e gestione profili

Le procedure di autenticazione forniscono automaticamente accesso alle risorse informatiche e ai dati necessari alle rispettive mansioni di assegnazione del ruolo nell’organizzazione.

Gli utenti sono tenuti al rispetto dei profili assegnati: ogni eventuale modifica deve essere richiesta e motivata.

Il Profilo Utente sarà disattivato in caso di cessazione del rapporto di lavoro o della collaborazione.

Successivamente alla cessazione del suddetto rapporto di lavoro o, inoltre, la documentazione informatica, la corrispondenza elettronica ed i documenti allegati archiviati in rete e sui supporti fissi (hard disk/server) o mobili (*storage*, cd, etc.) si intenderanno di esclusiva proprietà della scuola: quest'ultima pertanto potrà liberamente accedervi e/o utilizzarli nell'esercizio della propria attività e ei limiti delle finalità ad essa aderenti o per adempiere obblighi di legge.

Resta inteso che, anche successivamente alla cessazione del rapporto lavorativo, l'utente potrà esercitare i diritti previsti dalla legge con le modalità indicate nelle apposite informative.

All'Amministratore di Sistema potrà essere consentito l'accesso ai dati personali dell'utente (account di posta elettronica, file, ecc.), e ciò in caso di prolungata assenza o di impedimento dell'incaricato che renda indispensabili interventi sull'operatività e sulla sicurezza del sistema.

In tali ipotesi sarà comunque garantita la riservatezza dell'incaricato, informandolo tempestivamente dell'intervento effettuato e delle relative cautele.

Non è consentita la modifica delle caratteristiche impostate sul proprio PC, salvo autorizzazione.

Sezione III – Disciplina delle dotazioni

Ogni utilizzo dei personal computer e dispositivo dati in dotazione o in uso al collaboratore dovrà essere strettamente inerente all'attività lavorativa.

L'utente / collaboratore è ritenuto responsabile degli strumenti informatici al medesimo assegnati e deve custodirli con diligenza. Il dispositivo dovrà essere spento prima di lasciare gli uffici ed ogni qual volta si ravvisi la necessità di allontanarsi dal posto di lavoro dovrà essere attivata la protezione tramite password (ossia il c.d. "screen saver", blocco del computer con password di ripristino).

Tutti i computer forniti in dotazione, anche portatili o cd *tablet,* sono protetti da un apposito programma antivirus, periodicamente aggiornato. Qualsiasi anomalia o malfunzionamento del computer dovrà essere segnalata tempestivamente all'Amministratore di sistema o al dirigente responsabile.

I portatili utilizzati all'esterno devono essere custoditi in un luogo protetto per prevenirne il furto.

Qualora sia necessario memorizzare sui PC portatili dati considerati sensibili dalla legge, è obbligatorio l'utilizzo di tecnologie di protezione (es: crittografia, anonimizzazione, ecc.).

In caso di un prolungato periodo temporale in cui si è impossibilitati al collegamento con la rete scolastica si dovranno effettuare back up periodici su supporti rimovibili (Hard Disk esterni, Pen Drive, ecc.).

I supporti mobili, hard disk esterni, USB ”chiavette”, CD e DVD riscrivibili, memorie a stato solido, ecc. hanno come caratteristiche un ingombro e un peso contenuti; sono strumenti di uso comune ed in grado di supportare l’efficacia dell’infrastruttura solo se correttamente utilizzati.

I servizi di “*personal cloud*” sono generalmente costituiti da un software multipiattaforma, che offre un servizio di file hosting e sincronizzazione automatica di file tramite web (es: Dropbox, ICloud, Google Drive, WeTransfer, ecc.).

L’utilizzo sistemi di “personal storage” o di supporti rimovibili non è consentito, se non previa autorizzazione da parte dei responsabili della scuola e adeguata verifica della sicurezza degli stessi.

Inoltre:

- in caso di furto o smarrimento dispositivi rimovibili, gli utenti hanno l'obbligo di avvisare immediatamente il dirigente responsabile o l’ufficio competente;
- se un utente sospetta che sia stato effettuato un accesso non autorizzato ai dati, dovrà farsi carico di riferirlo immediatamente al dirigente;
- occorre dotare i dispositivi in ancorché autorizzati, agli utenti è consentito caricare sul o sui dispositivi rimovibili e sui sistemi di *personal storage* solamente i dati essenziali allo svolgimento del proprio lavoro;
- parola di adeguate procedure di autenticazione (es: password) per l’accesso alle informazioni;
- è proibito scaricare sui dispositivi in parola copie pirata di software, o contenuti illegali.

Tutti i dispositivi di archiviazione contenenti dati sensibili devono essere trattati con cautela al fine di evitare che il loro contenuto possa essere recuperato o cadere in mano a terzi non autorizzati.

La semplice cancellazione dei supporti non garantisce l’eliminazione dei dati in essi memorizzati: un esperto potrebbe infatti recuperare dati memorizzati anche dopo la loro cancellazione. Supporti magnetici o tabulati, contenenti dati sensibili devono essere custoditi in archivi, cassetti chiusi a chiave.

Per quanto riguarda i c.d. *mobile devices* (smartphone/tablet) eventualmente assegnati in dotazione al personale, quest’ultimo è avvertito di:

- non modificare le impostazioni di sistema;
- prestare attenzione all’utilizzo in luoghi pubblici in cui potrebbero essere intercettate informazioni; evitare di collegare lo strumento a dispositivi non scolastici;
- segnalare immediatamente eventuali anomalie;
- prestare attenzione alla custodia dello strumento e segnalare immediatamente lo smarrimento o il furto al responsabile.

Al fine di limitare i suddetti rischi, e nel rispetto delle cautele a tutela degli interessati, l’ufficio competente potrà avvalersi delle seguenti funzionalità:

- attivazione PIN della SIM Card
- attivazione di ulteriori procedure di autenticazione (ad applicazioni o supporti di memoria)
- impostazione di prestabiliti tempi di session time-out

- definizione di apposite politiche di back-up
- attivazione delle funzionalità di aggiornamento automatico dei sistemi operativi e dei programmi anti-malware
- attivazione delle procedure di remote-wiping da utilizzare in caso di smarrimento/furto del dispositivo
- attivazione delle funzionalità di cifratura automatica dei dati
- sistemi di controllo delle applicazioni installabili (c.d. white list)
- sistemi di blocco navigazione e tracciatura attività
- se necessario, sistemi di geolocalizzazione dello strumento

Nel caso in cui si conservino dei dati relativi al lavoro sul proprio smartphone o tablet sarà comunque indispensabile criptarli, sia che questi vengano custoditi nella memoria interna dello strumento sia che vengano archiviati su una memory card.

Inoltre è vietato l'utilizzo dello smarphone eventualemente messo a disposizione da parte della scuola per inviare o ricevere messaggi elettronici (SMS, MMS, WhatsApp, ecc.) di natura personale, o comunque non pertinenti rispetto all'attività lavorativa o alle finalità istituzionali della scuola.

L'eventuale uso promiscuo (per fini personali) dello smartphone intestato alla scuola (se presente) è consentito soltanto in caso di necessità o previa autorizzazione del rispettivo responsabile.

Non è consentito il collegamento alla rete wi-fi dell'istituto tramite strumenti personali, salvo che muniti di preventiva autorizzazione.

Si vieta di introdurre e utilizzare a scuola, in assenza di specifico assenso, personal computer o altre apparecchiature elettroniche personali.

Nel caso di utilizzo degli strumenti di lavoro, anche personali se usati eccezionalmente per finalità di lavoro, di fuori dei locali scolastici o presso la sede di terzi, ricordarsi di:

- Utilizzare un PIN o una password per proteggere uno smartphone della scuola
- Utilizzare PIN e password forti
- Criptare i dati conservati sugli smartphone
- Installare sugli smartphone dei software di sicurezza dedicati in modo da proteggere i device da virus e malware
- Chiudere le applicazioni che non si utilizzano (in questo modo non solo si limitano gli attacchi ma si incrementa anche la durata della batteria dello smartphone)
- Implementare la sicurezza degli smartphone anche con software di monitoraggio e di gestione dedicati
- Alcuni smartphone possono essere configurati utilizzando dei parametri personali di gestione così da impedire la visualizzazione, la copia o l'inoltro di dati personali da parte di estranei
- Spegnere il Bluetooth, il Wi-Fi e il GPS quando non vengono utilizzati
- Connettersi alla rete scolastica (dall'esterno, in out sourcing) tramite SSL VPN
- Considerare con la dovuta attenzione la possibilità di far connettere gli smartphone dei clienti o di altri dipendenti alla rete scolastica e informare il responsabile di tali eventualità.

In caso di furto smarrimento o furto, informare il responsabile e:

- Bloccare la linea
- Localizzare lo smartphone
- Bloccare o resettare lo smartphone a distanza
- Recuperare il codice IMEI (si ricorda che il codice IMEI (International Mobile Equipment Identity) è il DNA di un dispositivo, quel codice numerico di 15 cifre che permette di identificarlo in modo univoco. Recuperarlo è uno step essenziale per potersi poi rivolgere al proprio operatore telefonico o alla polizia per bloccare il telefono nel caso in cui non siate riusciti a farlo con il metodo indicato sopra.
- Denunciare il furto alle autorità
- Prevenire è meglio che curare (ricordarsi di fare i back up).

Sezione IV – Buone pratiche di gestione

Gli strumenti hardware necessari all'effettuazione di specifiche operazioni (dispositivi e card per la firma digitale, token per operazioni bancarie, ecc.) devono essere utilizzati esclusivamente dagli utenti espressamente identificati ed autorizzati. Tali utenti sono responsabili del corretto utilizzo di tali strumenti e devono preoccuparsi di:

- non consentirne l'accesso e l'utilizzo a soggetti non autorizzati;
- riporli alla fine dell'utilizzo (che deve essere il più possibile limitato nel tempo) nelle posizioni idonee;
- adottare tutti gli accorgimenti atti a prevenirne il furto o lo smarrimento.

Rientrano nelle medesime prescrizioni gli strumenti di registrazione degli accessi e delle presenze.

Tutti i documenti compresi quelli cartacei devono essere gestiti in modo da ridurre al minimo i tempi di permanenza al di fuori degli archivi o degli armadi o contenitori in dotazione.

Si rammenta che le stampe dimenticate o lasciate nella stampante o in luoghi limitrofi possono comportare la diffusione di dati e notizie, anche di carattere riservato. Per questo motivo occorre prestare la massima attenzione all'utilizzo delle stampanti, provvedendo se del caso alla distruzione di documenti non più necessari o stampati per errore.

La stampa dei dati dovrà avvenire solo se strettamente necessaria e andrà ritirata prontamente dai vassoi delle stampanti comuni. Sarà inloltre necessario prestare la massima attenzione all'eventuale riutilizzo di stampe (carta da riciclo): tale pratica è di norma autorizzata solo quando i documenti contengano dati non personali pubblici.

Le copie dei documenti vanno trattate, con riferimento alla tutela dei dati personali in esse contenuti, con la stessa diligenza riservata agli originali. Gli utenti sono tenuti a vigilare sull'accesso ai locali in cui operano da parte di personale non identificato o non autorizzato.
Massima attenzione dovrà essere posta per i documenti che si trovano in locali accessibili al pubblico. L'accesso agli archivi è consentito al personale a ciò espressamente autorizzato in via permanente od occasionale. Gli archivi devono essere mantenuti costantemente chiusi, compatibilmente con le esigenze di servizio.

Speciali e più rigorose cautele potranno essere adottato in considerazione della natura dei dati e delle informazioni trattate.

Sezione V – Collegamento ai sistemi da remoto (VPN)

L'accesso da remoto ai propri sistemi informativi mediante canali di comunicazione protetti VPN (Virtual Private Network, se presenti in istituto) potrà avvenire solo dietro autorizzazione, a seguito di richiesta motivata da parte dell'utente collaboratore per giustificate esigenze di lavoro.

Possono accedere da remoto all'infrastruttura IT tramite VPN solo gli utenti a cui siano state consegnate le apposite credenziali di accesso personali, e ciò esclusivamente per il periodo di tempo necessario all'espletamento dei propri compiti e previo rispetto del presente regolamento.

La scuola può comunque disattivare in qualsiasi momento le credenziali o disconnettere un accesso VPN, senza necessità di preventivo avviso, qualora la disattivazione sia necessaria all'integrità o al funzionamento dei propri servizi IT, oppure qualora vi sia fondato sospetto che l'Utente VPN abbia violato il presente Regolamento. Essa potrà inoltre utilizzare sistemi di monitoraggio della rete e dei sistemi per verificare la legittimità dell'operato dell'Utente VPN.

Sezione VI – Wi-fi scolastiche

Il collegamento alle reti wireless dell'istituto deve rispecchiare le modalità e le configurazioni di sicurezza prestabilite.

L'utilizzo delle suddette tecnologie deve rispettare le seguenti disposizioni:

- collegarsi alle reti wireless solamente mediante strumenti scolastici solo per fini lavorativi
- segnalare eventuali richieste di accesso alle reti wireless da parte di soggetti esterni (ospiti, consulenti, fornitori, ecc.).

- Sezione VII – Posta elettronica

La casella di posta elettronica e la navigazione in internet non possono essere utilizzate a fini personali o comunque estranei all'attività di lavoro o alle finalità istituzionali della scuola.

L'utente sarà in ogni caso direttamente ed esclusivamente responsabile dell'attività svolta attraverso la propria casella di posta.

L'utente non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, foto, video, audio, ecc.) messaggi che:

- possano danneggiare la reputazione e l'immagine della scuola;
- siano diffamatori, osceni, pornografici, offensivi, tali da recare danno o che possano essere considerati fonte di molestie o discriminazione religiosa, sessuale, razziale, politica;
- contengano pubblicità non istituzionale, manifesta, occulta o comunicazioni commerciali private;
- possano infrangere la legislazione vigente, in particolare quella sui diritti d'autore;

- contengano virus e/o altri codici dannosi, spamming (materiali indesiderati) o messaggi di natura ripetitiva (messaggi da diffondere).

L'utente è ritenuto responsabile della propria posta elettronica e si impegna a salvaguardare la riservatezza dei propri parametri di accesso, segnalando tempestivamente ogni circostanza che possa compromettere la segretezza della stessa.

L'utente deve prestare particolare attenzione alla sicurezza del dispositivo hardware eventualmente utilizzato per scaricare i messaggi di posta elettronica, soprattutto se si tratta di un dispositivo mobile (notebook, smartphone, tablet, ecc.), maggiormente soggetto a rischio di furto.

Sezione VIII – Internet

L'accesso ad Internet può essere effettuato esclusivamente:

- per ragioni strettamente attinenti all'attività lavorativa o alle finalità istituzionali della scuola, per il tempo strettamente e ragionevolmente necessario all'espletamento della suddetta;
- tramite il browser di navigazione preinstallato dall'ufficio IT, nel rispetto dei filtri di sicurezza preimpostati.

Non sono consentite le seguenti attività, se non autorizzate:

- effettuare di qualunque genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili;
- partecipare a «forum», «chat line», bacheche elettroniche e «social network» anche utilizzando pseudonimi (o nicknames);
- prelevare e memorizzare siti Internet (download) o software gratuiti (freeware) e (shareware);
- l'invio (upload) di file e/o dati verso Internet, fatta eccezione per quanto strettamente attinente alla propria attività lavorativa e nell'esercizio autorizzato della medesima;
- forzare i filtri automatici di cui al punto precedente al fine di accedere a siti non consentiti.

Sezione IX – Controlli e disposizioni generali

Tutti gli strumenti e le strutture citate nel presente documento, per le finalità indicate, pogtranno consentire l'archiviazione di dati relativi al loro utilizzo (log-management), che possono ricondurre a comportamenti dell'utente.

L'attività di verifica è effettuata esclusivamente da soggetti appositamente nominati ed istruiti, solo per fini di sicurezza, sviluppo/manutenzione infrastruttura/ controllo dei costi.

Nell'effettuare eventuali controlli sull'uso degli strumenti elettronici saranno evitate interferenze ingiustificate sui diritti e sulle libertà fondamentali dei collaboratori, rispettando i principi di pertinenza e di non eccedenza. Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato evitato con preventivi accorgimenti tecnici, la scuola potrà adottare misure atte a consentire l'individuazione di comportamenti anomali o scorretti.

Il controllo anonimo si conclude con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti scolastici e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. Secondariamente l'avviso sarà circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati. Resta fermo il diritto della scuola e del dirigente di effettuare controlli identificativi quando ciò sia dettato da:

- riscontri di mancato rispetto dei regolamenti;
- oggettivi indizi di commissione di reato;
- specifiche richieste delle forze dell'ordine;
- segnalazione di circostanze sospette da parte della struttura di protezione della rete.

L'inosservanza delle regole contenute nel presente documento comporterà l'immediata revoca delle autorizzazioni ad accedere alla Rete Informatica ed ai servizi/programmi precedentemente autorizzati, fatte salve le sanzioni previste dalla normativa vigente.

Il Dirigente Scolastico
Antonia Lusardi