Ministero dell'Istruzione e del Merito
ISTITUTO COMPRENSIVO STATALE "GATTI – MANZONI-AUGRUSO"
Scuola Secondaria di I grado – Scuola Primaria – Scuola dell'Infanzia
Via G. Amendola s.n.c. – 88046 – Lamezia Terme (CZ) Tel. 0968-462500
Mail istituzionale: czic84400q@istruzione.it – mail PEC: czic84400q@pec.istruzione.it
COD. MECC. CZIC84400Q – C.F. 92002540794 – COD. FATT. UF7F01

DIRETTIVA PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI ALL'INTERNO DELL'ISTITUZIONE SCOLASTICA (E-POLICY)

Aggiornato al DPR n.81 del 13/06/2023 - Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165».

PREMESSA

1.FINALITÀ E DESTINATARI

La presente direttiva ha efficacia su tutti gli Utenti (dipendenti/alunni/genitori/collaboratori) dell'istituzione scolastica IC Lamezia Gatti-Manzoni-Augruso.

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet da Personal Computer, tablet e smartphone, espone la Scuola e gli Utenti a rischi di natura patrimoniale, oltre alle responsabilità penali connesse alla violazione di specifiche disposizioni di legge, creando evidenti problemi alla sicurezza ed all'immagine della Scuola stessa.

Risulta, pertanto, necessario, a tutela degli utenti e dell'istituzione scolastica, fornire direttive mirate a garantire il corretto uso delle strumentazioni informatiche e digitali, al fine di prevenire ed evitare comportamenti, anche inconsapevoli, che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Regolamento Europeo sulla protezione dei dati.

La presente direttiva verrà portata a conoscenza anche di collaboratori, consulenti o altri incaricati esterni (es. incaricati software house, incaricati dei professionisti di cui si avvale

la Scuola, etc.), studenti, famigliari che venissero autorizzati a far uso di strumenti tecnologici della Scuola o ad accedere alla rete informatica della scuola e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, il presente regolamento entra a far parte, per quanto occorra, del Codice disciplinare della scuola.
Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Dirigenza scolastica.

2. CAMPO DI APPLICAZIONE

La presente direttiva regolamenta il corretto uso di tutti i dispositivi informatici, computer, pc, tablet, mobile devices, utilizzati nella scuola.

3. UTILIZZO DEL PERSONAL COMPUTER

3.1 Il Personal Computer affidato all'utente deve essere usato solo come strumento di lavoro. Ogni utilizzo non inerente all'attività scolastica è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.
Il personal computer dato in affidamento all'utente permette l'accesso alla rete della Scuola solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4.
3.2 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 pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone la Scuola a responsabilità civili.
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 penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico della Scuola, come disposta dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.
3.3 Il Personal Computer deve essere spento ogni sera prima di lasciare i locali della Scuola. In caso di suo inutilizzo, il pc deve essere bloccato e l'utente si deve scollegare dal pc: 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 E ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

4.1 Le credenziali di autenticazione (utente e password) per l'accesso alla rete vengono assegnate dal DS o dipendenti da lui incaricati.
4.2 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'utente con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Dirigente Scolastico.
È necessario procedere alla modifica della parola chiave a cura dell'utente al primo utilizzo oppure in caso di perdita di qualità della stessa. Qualora venga scelta una parola chiave particolarmente complessa, può anche non essere modificata periodicamente.

Si ricorda che quando si utilizza un sistema condiviso con altri utenti, non si deve mai memorizzare alcuna password quali ad esempio quelle del registro elettronico o dell'account Google: memorizzando la password, altri utenti potrebbero facilmente accedere ai vostri dati personali.

5. UTILIZZO DELLA RETE INFORMATICA

Le parole 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 della Scuola sono aree di condivisione di informazioni e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività scolastica non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e back up da parte del personale addetto. Si ricorda che tutti i dischi o altre unità di memorizzazione locali non sono soggette a salvataggio da parte del personale incaricato del Servizio. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

Il personale addetto 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.

6. UTILIZZO DI ALTRI DISPOSITIVI ELETTRONICI

Tutti i dispositivi elettronici forniti in dotazione dalla Scuola devono considerarsi materiale scolastico: ne viene concesso l'uso esclusivamente per lo svolgimento delle attività scolastiche, non essendo quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività scolastiche. Fra i dispositivi in questione vanno annoverati i telefoni della scuola, PC portatili, tablet, telefoni cellulari, smartphone, etc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere alla rete della Scuola o di condividere documenti, dati e materiali ivi conservati e/o trattati.

L'utente resta responsabile del singolo dispositivo assegnato e deve custodirlo con diligenza sia durante trasferte e spostamenti sia durante l'utilizzo nel luogo di lavoro; va sempre adottata ogni cautela per evitare danni o sottrazioni.

Viene infine disposto il divieto di utilizzo per fini personali di strumenti della scuola, per spedire o per ricevere documentazione, e/o di fotocopiatrici della scuola, salva diversa esplicita autorizzazione da parte del Dirigente Scolastico.

7. UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

7.1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how della scuola, 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.

7.2 L'utente resta, in ogni caso responsabile della custodia dei supporti e dei dati della scuola in essi contenuti; in particolare, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

Nel caso di dispositivi elettronici, con riferimento in particolare a PC portatili, tablet ed altri dispositivi sui quali possano venir salvati documenti, dati ed altro materiale, dovrà farsi particolare attenzione al salvataggio in opportuni supporti esterni di tale materiale oppure alla sua rimozione effettiva prima della riconsegna del dispositivo.

7.3 In caso di smarrimento di una chiavetta USB contenente dati personali, avvisare immediatamente il Dirigente scolastico e il Responsabile della protezione dei dati (DPO).

8. UTILIZZO DELLA POSTA ELETTRONICA

8.1 La casella di posta elettronica assegnata all'utente è uno strumento da utilizzarsi solo per le attività scolastiche. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

È fatto divieto di utilizzare le caselle di posta elettronica della scuola per motivi diversi da quelli strettamente legati all'attività scolastica. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività scolastica;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, lo si dovrebbe comunicare immediatamente al Dirigente Scolastico. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.2 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili o non costituenti corrispondenza scolastica e soprattutto allegati ingombranti. In caso di cessazione del rapporto con La Scuola, quest'ultima provvederà, senza preavviso, alla eliminazione dell'account di posta e dei relativi messaggi ivi contenuti.

È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web non conosciuti).

8.3 L'indirizzo e-mail è un dato personale e non va rivelato ad alcuno se non necessario. Nel caso di invio di comunicazioni e/o inviti per e-mail ai membri dei gruppi di lavoro per l'inclusione non si devono quindi mai mettere gli indirizzi e-mail dei destinatari in chiaro, ma l'invio deve essere effettuato in modo che per nessun destinatario siano visibili gli indirizzi e-mail degli altri, a tutela della privacy.

L'indirizzo e-mail viene cancellato alla cessazione del rapporto con la scuola e tutti i dati contenuti vengono di conseguenza eliminati.

8.4 L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può' in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale. Il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'amministrazione di appartenenza. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.

8.5 È vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.

9. NAVIGAZIONE IN INTERNET E WIFI

9.1 Le seguenti disposizioni sono valide sia per chi utilizza strumenti scolastici che strumenti personali. Durante l'utilizzo di internet all'interno della scuola è assolutamente proibita la navigazione per motivi diversi da quelli strettamente legati all'attività scolastica. L'utilizzo di tutte le reti WiFi presenti presso la Scuola è limitato agli utenti autorizzati. A tale scopo si precisa che l'utilizzo di qualsiasi rete WiFi disponibile è possibile solo a seguito di digitazione di specifiche credenziali che vengono assegnate dal Dirigente scolastico o personale incaricato. È assolutamente vietato comunicare a terzi non autorizzati e non facenti parte della comunità scolastica la password o le credenziali di accesso alle reti WiFi scolastiche.

9.2 Non è consentito l'accesso a siti e servizi che prevedano un traffico di dati sulla rete tali da pregiudicare il buon funzionamento della medesima.

9.3 Durante l'utilizzo della rete internet è vietato:

- svolgere qualunque attività che sia in contrasto con la normativa italiana ed europea;
- accedere a siti che per contenuti ed immagini siano in contrasto con le finalità servizio e/o illegali (siti pedofili, pornografici, che ispirano alla violenza, al razzismo, ecc.);
- inviare messaggi di posta secondo modalità indiscriminate (spamming);
- svolgere qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno esterno pubblico o privato
- usare meccanismi o strumenti di qualsiasi natura atti ad eludere i sistemi di protezione da copia abusiva del software, a rivelare password, ad identificare eventuali vulnerabilità della sicurezza dei vari sistemi, a decriptare file crittografati o a compromettere la sicurezza della rete in qualsiasi modo.

L'utente è direttamente responsabile delle attività svolte durante la connessione a Internet: le conseguenze penali e civili
derivanti da un uso fraudolento della medesima rete e ogni responsabilità civile e penale è in capo ai singoli utilizzatori della rete Internet.

10. PROTEZIONE ANTIVIRUS

Il sistema informatico della Scuola è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico della scuola mediante virus o mediante ogni altro software aggressivo.

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

Ogni dispositivo magnetico di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al Dirigente Scolastico.

11. PARTECIPAZIONI A SOCIAL MEDIA

11.1 L'utilizzo dei social media ufficiali della Scuola – quali Facebook™, Twitter™, Linkedin™, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dalla Dirigenza attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti.

11.2 Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, La Scuola ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio della scuola, anche immateriale, quanto i propri collaboratori e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione dal Titolare, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali.
11.3 La condivisione dei contenuti nei social media deve sempre rispettare e garantire i diritti dei soggetti coinvolti. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e
dei diritti d'autore, sia di terzi che della Scuola.
11.4 L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori della scuola e di studenti, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi della scuola, se non con il preventivo consenso della Dirigenza.
11.5 L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificamente verso la Scuola, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito della scuola.
Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla pubblica amministrazione di appartenenza. In ogni caso, il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.
11.6 Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'amministrazione e in difformità alle disposizioni di cui al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità attribuibili direttamente alla pubblica amministrazione di appartenenza.
In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.
Al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche

12. DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure adeguate di sicurezza dei dati personali.

In caso di rapporto di lavoro, gli strumenti tecnologici considerati nella presente direttiva costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970; conseguentemente, le informazioni raccolte sulla base di quanto indicato nella direttiva possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico della scuola ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti, fermo restando il rispetto della normativa in materia di protezione dei dati personali (GDPR 2016/679).

13. ACCESSO AI DATI TRATTATI DALL'UTENTE

Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio,
aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi della scuola (ad esempio, verifica costi di connessione a Internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività degli utenti, è facoltà della Direzione della scuola, tramite il personale incaricato o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy e delle procedure, a tutti gli strumenti informatici della scuola e ai documenti ivi contenuti.

14. ALTRE DISPOSIZIONI

E' vietato salvare sul personal computer e sul server della scuola per scopi personali files contenenti dati ritenuti sensibili, quali ad esempio copie delle buste paga (dipendenti) o altri dati sensibili quali esami, visite mediche, ecc. in qualsiasi formato.

La riservatezza dei dati personali è un valore per La Scuola ed occorre quindi che tutti gli attori, interni ed esterni, siano consapevoli che è vietato comunicare ad estranei contatti e altri dati patrimonio della scuola.

La presente direttiva potrà essere soggetta a periodica revisione.

Il Dirigente Scolastico
Dott.ssa Antonella Mongiardo
Firmato digitalmente