GDPR SCUOLA
LO STAFF TECNICO DEL DIRIGENTE

Oggetto: Istruzioni per l'utilizzo dell'indirizzo di posta elettronica istituzionale e la gestione delle credenziali di accesso

A tutto il personale docente e ATA

Le presenti istruzioni hanno lo scopo di fornire regole chiare e vincolanti per la corretta gestione e l'utilizzo dell'indirizzo di posta elettronica istituzionale (con dominio @[nomeistituto].edu.it) assegnato a ciascun docente e al personale ATA da parte della Scuola.

Tale strumento è fondamentale per le comunicazioni ufficiali, lavorative, la didattica e il corretto funzionamento delle attività scolastiche.

Un uso consapevole e sicuro degli strumenti informatici è essenziale per proteggere i dati personali e le informazioni dell'istituzione scolastica, in conformità con la normativa vigente in materia di protezione dei dati (Regolamento UE 2016/679 - GDPR) e le più recenti indicazioni del Garante per la Protezione dei Dati Personali e del Codice di Comportamento dei Dipendenti Pubblici (D.P.R. n. 62/2013).

1. Natura e finalità dell'indirizzo di posta elettronica istituzionale

L'indirizzo di posta elettronica istituzionale è uno strumento di lavoro di proprietà della Scuola. È assegnato al singolo dipendente per l'espletamento delle proprie funzioni e per tutte le comunicazioni di carattere professionale e di servizio.

È da utilizzarsi esclusivamente per le seguenti finalità:

- Comunicazioni tra il personale scolastico, la dirigenza e gli uffici di segreteria.
- Comunicazioni con studenti e famiglie, attraverso i canali e le modalità ufficiali stabilite dall'Istituto.
- Iscrizione e accesso a piattaforme per la Didattica Digitale Integrata (DDI) autorizzate dalla scuola.
- Invio e ricezione di documentazione attinente all'attività amministrativa, didattica e progettuale.
- Comunicazioni con enti, associazioni e altre istituzioni per attività legate alla funzione e al ruolo rivestito.

È severamente vietato l'utilizzo dell'account di posta istituzionale per scopi personali, privati, commerciali o per attività che non siano strettamente correlate al servizio.

2. Gestione delle credenziali di accesso (username e password)

Le credenziali di accesso (username e password) sono strettamente personali, riservate e non cedibili a terzi. La loro custodia è di esclusiva responsabilità del docente assegnatario.

Si forniscono le seguenti istruzioni vincolanti per la gestione della password:

- **Primo accesso e modifica obbligatoria:** Al primo accesso, è obbligatorio modificare la password provvisoria fornita dall'amministratore di sistema / animatore digitale.
- **Complessità della password:** La password deve essere "robusta", ovvero composta da almeno 12/15 caratteri, includendo una combinazione di lettere maiuscole, lettere minuscole, numeri e caratteri speciali (es. !, ?, @, #, $).
- **Periodicità del cambio:** È buona norma modificare la propria password a intervalli regolari (almeno ogni 90 giorni).
- **Divieto di condivisione:** È assolutamente vietato comunicare la propria password ad altri, inclusi colleghi, personale tecnico o superiori. Nessun operatore dell'istituto è autorizzato a richiedere la password.
- **Conservazione sicura:** Non scrivere la password su post-it, agende o altri supporti facilmente accessibili. Evitare di salvarla in modo non protetto su dispositivi o browser.

3. Norme di comportamento e sicurezza informatica

Per garantire la sicurezza dell'infrastruttura informatica e la protezione dei dati, ogni dipendente è tenuto a rispettare le seguenti norme:

- **Riconoscere il Phishing:** Diffidare di email inattese che richiedono di cliccare su link sospetti, di scaricare allegati o di inserire le proprie credenziali su pagine web non conosciute. L'Istituto non richiederà mai le credenziali di accesso via email. In caso di dubbi, contattare l'animatore digitale o la segreteria prima di compiere qualsiasi azione.
- **Gestione degli allegati:** Prestare la massima attenzione nell'aprire allegati provenienti da mittenti sconosciuti o con un oggetto sospetto. Assicurarsi che il proprio dispositivo sia dotato di un software antivirus aggiornato.
- **Utilizzo su dispositivi personali:** Qualora si acceda alla posta istituzionale da dispositivi personali (PC, tablet, smartphone), è responsabilità del dipendente assicurarsi che tali dispositivi siano adeguatamente protetti da password o PIN di sblocco e da software di sicurezza.

- **Utilizzo su dispositivi condivisi di proprietà della Scuola:** Nel caso in cui il dipendente accede alla propria email tramite pc condivisi della Scuola deve sempre ricordarsi si effettuare il log out e non deve mai salvare le proprie password di accesso sul dispositivo.
- **Accesso da dispositivi sicuri:** Evitare di accedere alla propria casella di posta da computer pubblici (es. internet point, hotel) o reti Wi-Fi non protette.
- **Comunicazioni massive:** L'invio di comunicazioni a un numero elevato di destinatari (es. a tutti i genitori di una classe) deve avvenire utilizzando il campo "Ccn" (Copia Conoscenza Nascosta) per proteggere gli indirizzi email dei singoli.
- **Linguaggio e contenuti:** Tutte le comunicazioni devono utilizzare un linguaggio consono, rispettoso e professionale. È vietato inviare messaggi a carattere offensivo, discriminatorio o che possano ledere l'immagine dell'istituzione scolastica.

4. Procedura in caso di smarrimento o compromissione delle credenziali

In caso di smarrimento della password o di sospetto che il proprio account sia stato violato (es. ricezione di avvisi di accessi anomali, invio di email non autorizzate dal proprio account), il dipendente deve:

1. **Segnalare immediatamente** l'accaduto all'Animatore Digitale o agli uffici di segreteria.
2. **Procedere, se possibile, al cambio immediato della password.**
3. **Non rispondere a eventuali richieste di riscatto o di informazioni personali.**

L'Istituto provvederà a resettare la password e a fornire nuove credenziali temporanee con la massima urgenza.

5. Disattivazione dell'account

L'account di posta elettronica istituzionale verrà disattivato al termine del rapporto di lavoro con questo Istituto. Il dipendente è tenuto a salvare e consegnare, secondo le modalità che verranno indicate, tutta la documentazione di carattere lavorativo presente nell'account prima della cessazione del servizio.

La violazione delle presenti disposizioni potrà comportare, a seguito di formale procedura di contestazione, l'applicazione di sanzioni disciplinari, in conformità a quanto previsto dalla normativa vigente.