

## AVVISO N. 85

**Agli studenti  
Al personale Docente  
Al personale ATA  
Al DSGA**

C.P.I.A. 1 - PRATO Prot. 0001191 del 13/05/2020 (Uscita)
--

### **Oggetto: Funzionamento account istituzionale “cpiaprato.edu.it”**

Nell’ottica di favorire lo sviluppo delle competenze digitali, la creazione e condivisione di risorse e documentazione didattica, il CPIA ha attivato per ogni studente e dipendente un servizio di posta elettronica che Google mette gratuitamente a disposizione delle scuole e delle università, con dominio *cpiaprato.edu.it*.

L’obiettivo di questa iniziativa è ottimizzare, attraverso le tecnologie di rete, l’attività didattica e la circolazione delle informazioni interne, come comunicazioni, documentazione e didattica tramite l’uso di applicazioni specifiche.

L’utilizzo della posta elettronica, insieme agli applicativi della *G-Suite*, consentono di gestire in modo efficace il flusso informativo all’interno dell’istituto attraverso alcune funzionalità principali. Tale piattaforma offre due categorie di servizi:

- *Gmail* per l’assegnazione di casella di posta con spazio illimitato;
- *Calendar* per la gestione dell’agenda;
- *Classroom* per la creazione e gestione di classi virtuali;
- *Drive* per l’archiviazione e condivisione di documenti;
- *Documenti, Fogli, Presentazioni, Moduli* per creare documenti, condividerli e modificarli;
- *Talk/Hangouts* per stabilire comunicazioni in tempo reale, creare webinar/videolezioni/riunioni.

Si ricorda che l’utilizzo del servizio di posta elettronica istituzionale è consentito solo per ragioni lavorative (personale) o di studio (studenti).

Tutti gli utenti devono valutare attentamente, prima di aprirli, i messaggi che provengono sulla propria casella di posta elettronica. Nel caso di mail di dubbia provenienza, gli allegati non dovranno essere aperti.

#### **Non è consentito:**

- 1) Utilizzare la posta elettronica istituzionale per motivi non attinenti alle mansioni assegnate;
- 2) Utilizzare l’indirizzo di posta elettronica istituzionale per la partecipazione a dibattiti, forum e mailing-list, salvo specifica autorizzazione in tal senso da parte del responsabile;

- 3) Aprire gli allegati di non comprovata origine in assenza di software antivirus aggiornato sulla propria postazione di lavoro;
- 4) Effettuare chiamate a link contenuti all'interno di messaggi a meno di comprovata sicurezza sul contenuto dei siti richiamati;
- 5) Rispondere ad e-mail pervenute da mittenti sconosciuti. Nel dubbio si suggerisce di cancellarle preventivamente;
- 6) Utilizzare il servizio di posta per inoltrare giochi, scherzi, barzellette, appelli e petizioni e altre e-mail che non siano di lavoro;
- 7) Allegare al testo delle comunicazioni materiale insicuro o file di dimensioni eccessive.
- 8) Prestare particolare attenzione ai messaggi di phishing, ossia messaggi di posta contenenti link a siti che mirano ad estorcere le credenziali di accesso ai sistemi informatici.

Si chiede ai docenti di dare massima diffusione del seguente avviso a tutti gli studenti.

Prato, 12/05/2020

Il Dirigente Scolastico  
Dott. Philipp Botes