



*Ministero dell'Istruzione e del Merito*  
*Ufficio Scolastico Regionale per il Lazio*  
**Liceo Scientifico Statale "G. KEPLERO"**

Cod. Mecc. RMPS19000T - C.F. 80230950588 - Distr. 23° - Sede centrale: Via Silvestro Gherardi, 87/89 - 00146 Roma  
Via Avicenna, snc - 00146 Roma - Tel. 06121123925 - Succursale: Via delle Vigne, 156 - 00148 Roma – Tel. 06121126685  
Sito web: [www.liceokepleroroma.edu.it](http://www.liceokepleroroma.edu.it) - E-mail: [rmps19000t@istruzione.it](mailto:rmps19000t@istruzione.it) - [succursale@liceokepleroroma.edu.it](mailto:succursale@liceokepleroroma.edu.it)

## **REGOLAMENTO PER L'ACCESSO ALLA RETE DI ISTITUTO**

### **Articolo 1. Descrizione del servizio**

Il Liceo Scientifico "Giovanni Keplero" mette a disposizione dei propri dipendenti e studenti (di seguito denominati "utenti") l'accesso alla rete di Istituto, al fine di promuovere l'innovazione didattica e migliorare l'efficienza dei servizi amministrativi. Il presente Regolamento disciplina le condizioni di utilizzo della rete di Istituto e delle risorse ad essa connesse e definisce le modalità di accesso per la fruizione del servizio.

### **Articolo 2. Gestione del servizio**

1. Il servizio è gestito da un Assistente Tecnico dipendente dell'Amministrazione, il quale esercita la funzione di amministratore di sistema in riferimento alla gestione e manutenzione della rete.
2. L'amministratore di sistema si occupa, in cogestione con altri soggetti affidatari di servizi presso l'Istituto, della creazione e gestione degli account utente, del monitoraggio della sicurezza della rete e dell'assistenza tecnica agli utenti.

### **Articolo 3. Modalità di accesso**

1. L'accesso alla rete avviene mediante credenziali personali (username e password) fornite dall'amministratore di sistema ovvero messe a disposizione dall'Istituto.
2. La password iniziale è temporanea e deve essere modificata al primo accesso dall'utente.
3. Le credenziali sono strettamente personali e non cedibili.
4. L'utente è responsabile di tutte le attività svolte mediante il proprio account.
5. È vietato l'accesso alla rete mediante credenziali di altri utenti o attraverso postazioni non autorizzate.

### **Articolo 4. Postazioni autorizzate**

1. Per il personale docente:
  - ✓ PC nelle aule
  - ✓ PC nei laboratori fissi e mobili
  - ✓ PC in sala insegnanti
  - ✓ Dispositivi personali eventualmente forniti dall'Istituto
2. Per il personale ATA:
  - ✓ PC degli uffici
  - ✓ PC dedicati in locali specifici
  - ✓ Dispositivi personali eventualmente forniti dall'Istituto
3. Per gli studenti:
  - ✓ PC nelle aule
  - ✓ PC nei laboratori fissi e mobili

### **Articolo 5. Attività consentite**

1. Per il personale:
  - ✓ Attività connesse alla propria mansione e strettamente legate all'attività lavorativa
  - ✓ Consultazione e gestione della casella di posta istituzionale secondo il relativo Regolamento

- ✓ Utilizzo di piattaforme e servizi digitali per la didattica e l'Amministrazione
- 2. Per gli studenti:
  - ✓ Attività didattiche sotto la supervisione dei docenti
  - ✓ Utilizzo della posta elettronica istituzionale secondo il relativo Regolamento
  - ✓ Accesso a piattaforme e servizi digitali per la didattica

#### **Articolo 6. Attività vietate**

È espressamente vietato:

1. Accedere a siti con contenuti pornografici, violenti, o comunque non pertinenti alle attività istituzionali
2. Utilizzare piattaforme di streaming non autorizzate
3. Scaricare o condividere materiale protetto da diritto d'autore
4. Svolgere attività che violino la privacy degli utenti o le disposizioni di legge
5. Utilizzare la rete per attività commerciali o personali
6. Installare software non autorizzato sulle postazioni dell'Istituto
7. Modificare le configurazioni di rete o di sistema delle postazioni

#### **Articolo 7. Monitoraggio e sanzioni**

1. L'amministratore di sistema può monitorare le attività sulla rete per garantire la sicurezza e il rispetto del presente Regolamento.
2. In caso di violazione delle norme, il Liceo "Keplero" potrà:
  - ✓ Sospendere o revocare l'accesso alla rete
  - ✓ Applicare sanzioni disciplinari secondo i Regolamenti vigenti
  - ✓ Segnalare alle autorità competenti eventuali attività illecite
  - ✓ Richiedere il risarcimento di eventuali danni causati

#### **Articolo 8. Norme di Sicurezza Informatica**

1. Password e Credenziali:
  - ✓ Utilizzare password di almeno nove caratteri
  - ✓ Combinare caratteri alfabetici, numerici e caratteri speciali
  - ✓ Evitare riferimenti personali (nome, cognome, date di nascita)
  - ✓ Non utilizzare la stessa password per servizi diversi
  - ✓ Modificare le credenziali con cadenza trimestrale
  - ✓ Non memorizzare le password sui dispositivi o browser
  - ✓ Non condividere mai le proprie credenziali
2. Uso della Posta Elettronica:
  - ✓ Non aprire allegati da mittenti sconosciuti
  - ✓ Verificare la legittimità dei mittenti che sembrano istituzionali
  - ✓ Non cliccare su link sospetti
  - ✓ Non utilizzare la mail istituzionale per servizi non lavorativi
  - ✓ Segnalare immediatamente attività sospette
3. Utilizzo dei Dispositivi:
  - ✓ Non installare software non autorizzato
  - ✓ Mantenere aggiornato il sistema operativo
  - ✓ Utilizzare solo sistemi operativi con supporto attivo
  - ✓ Eseguire scansioni antivirus sui dispositivi esterni
  - ✓ Effettuare sempre il logout dai servizi al termine dell'utilizzo
  - ✓ Non lasciare incustodite le postazioni sbloccate
4. Sicurezza della Rete:
  - ✓ Utilizzare solo connessioni Wi-Fi protette
  - ✓ Non modificare le configurazioni di rete impostate
  - ✓ Segnalare anomalie all'amministratore di sistema
  - ✓ Non utilizzare reti Wi-Fi non sicure

#### 5. Gestione dei Dati:

- ✓ Non memorizzare dati personali sui dispositivi della scuola
- ✓ Segnalare immediatamente potenziali violazioni dei dati (*data breach*)
- ✓ Utilizzare solo dispositivi di archiviazione esterni verificati
- ✓ Effettuare scansioni antivirus prima di collegare dispositivi esterni

#### Articolo 9. Responsabilità

1. Ogni utente è personalmente responsabile dell'utilizzo del proprio account e delle attività svolte sulla rete.
2. L'utente si impegna a:
  - ✓ Mantenere riservate le proprie credenziali
  - ✓ Segnalare immediatamente eventuali anomalie o violazioni della sicurezza
  - ✓ Rispettare le norme vigenti in materia di privacy e diritto d'autore
  - ✓ Utilizzare la rete in modo etico e responsabile

#### Articolo 10. Segnalazione incidenti

1. Gli utenti sono tenuti a segnalare immediatamente al dirigente scolastico e all'amministratore di sistema:
  - ✓ Sospette violazioni della sicurezza
  - ✓ Accessi non autorizzati
  - ✓ Furti o perdite di dispositivi
  - ✓ Anomalie nel funzionamento dei sistemi
  - ✓ Potenziali violazioni dei dati personali (*data breach*)
2. In caso di dubbi su operazioni da effettuare sui sistemi informatici o sospetti di violazione, gli utenti devono rivolgersi all'amministratore di sistema.

#### Articolo 11. Norme finali

1. Il presente Regolamento si integra con gli altri Regolamenti vigenti presso l'Istituto, con tutti i documenti pubblicati nella sezione "Gestione della sicurezza informatica" del sito web istituzionale e, in particolare, con il Disciplinary interno per l'utilizzo di Internet e della posta elettronica da parte del personale scolastico.
2. Il Liceo "Keplero" si riserva il diritto di modificare in qualsiasi momento il presente Regolamento e i rimanenti documenti pubblicati nella sezione "Gestione della sicurezza informatica", dandone comunicazione agli utenti.
3. Per quanto non espressamente previsto nel presente Regolamento, si rinvia alla normativa vigente.

*Il presente Regolamento è stato approvato dal Consiglio di Istituto con Delibera n. 15 dell'8 gennaio 2026.*