

[NOME ISTITUTO SCOLASTICO]

[Città (Prov.)]

VADEMECUM

Uso corretto degli account scolastici Google Workspace
e dei PC condivisi nei laboratori

Anno Scolastico ____/____

Destinatari:	Tutti gli studenti, i docenti e il personale dell'istituto
Redattore:	[Referente ICT / Animatore Digitale]
Approvazione:	Dirigente Scolastico
Data:	A.S. ____/____

*Template originale a cura di Davide Bertolino — davidebertolino.it
Rilasciato per uso gratuito da parte di qualsiasi istituto scolastico.*

1. Premessa

L'istituto mette a disposizione di ogni studente e di ogni membro del personale un account Google Workspace for Education con dominio @[dominio-scolastico].edu.it. Questo account consente l'accesso a Gmail, Google Drive, Google Classroom e a tutti i servizi della suite Google per uso didattico e istituzionale.

L'account scolastico è uno strumento di lavoro e di studio. Il suo utilizzo comporta responsabilità precise, sia sotto il profilo della sicurezza informatica sia sotto il profilo giuridico. Il presente vademecum fornisce regole chiare e indicazioni pratiche affinché ogni utente possa operare in sicurezza, tutelando sé stesso e gli altri.

Attenzione

L'account scolastico @[dominio-scolastico].edu.it è personale e non cedibile. Ogni attività compiuta con il tuo account è registrata nei log di sistema e risulta riconducibile a te. Se qualcuno utilizza il tuo account senza autorizzazione, le conseguenze ricadono in prima istanza sul titolare dell'account.

2. Il tuo account scolastico

2.1 Cosa include

- Un indirizzo email @[dominio-scolastico].edu.it con accesso a Gmail.
- Spazio su Google Drive per documenti, compiti e materiali didattici.
- Accesso a Google Classroom, Google Meet, Google Calendar e alle altre app della suite.
- Possibilità di autenticazione (login) sui PC dei laboratori e sui dispositivi scolastici.

2.2 Cosa NON è consentito

- Condividere la propria password con altri, nemmeno con compagni di classe o amici.
- Utilizzare l'account di un altro studente o di un docente, anche con il suo consenso.
- Utilizzare l'account scolastico per scopi personali non legati alla didattica (acquisti online, iscrizione a social network, gaming).
- Inviare messaggi offensivi, minacciosi o contenenti materiale inappropriato.
- Tentare di accedere ai dati o alla posta di altri utenti.
- Memorizzare la password dell'account scolastico su dispositivi non propri.

3. La password: la tua prima difesa

La password è l'unico elemento che protegge il tuo account da accessi non autorizzati. Una password debole o condivisa equivale a lasciare la porta di casa aperta.

3.1 Regole per una password sicura

- Almeno 12 caratteri, combinando lettere maiuscole, minuscole, numeri e simboli.
- Non usare informazioni personali facilmente indovinabili: nome, cognome, data di nascita, nome del proprio animale domestico.
- Non usare la stessa password che utilizzi per i tuoi account personali (Instagram, TikTok, gaming, ecc.).
- Cambia la password almeno una volta a quadrimestre, o immediatamente se sospetti che qualcuno l'abbia vista.

3.2 Cosa fare se pensi che qualcuno conosca la tua password

1. Cambiala immediatamente da myaccount.google.com → Sicurezza → Password.
2. Controlla “Attività recenti per la sicurezza” per verificare accessi sospetti.
3. Avvisa il tuo docente o gli amministratori del dominio scolastico il prima possibile.
4. Se hai usato la stessa password anche su altri servizi, cambiala ovunque.

4. Uso dei PC condivisi nei laboratori

Regola d'oro

Ogni volta che finisci di usare un PC di laboratorio, ESCI da tutti i tuoi account. Nessuna eccezione.

I PC dei laboratori sono condivisi tra decine di studenti ogni giorno. Lasciare una sessione aperta significa consegnare il proprio account a chiunque si sieda dopo di te.

4.1 Prima di iniziare a lavorare

1. Verifica che il browser non abbia sessioni aperte di altri utenti. Se trovi un account altrui ancora collegato, NON utilizzarlo: esci dalla sessione e avvisa un docente.
2. Apri una finestra di navigazione in incognito (Ctrl+Shift+N su Chrome) se vuoi evitare che le tue credenziali vengano salvate sul PC. Questa è la modalità più sicura per lavorare su un PC condiviso.
3. Se non usi la modalità incognito, non selezionare mai “Ricorda password” o “Resta collegato” quando il browser lo chiede.

4.2 Mentre lavori

- Non lasciare il PC incustodito con la sessione aperta, nemmeno per pochi minuti. Se devi allontanarti, blocca il PC (Windows+L) o esci dall'account.
- Non aprire link sospetti ricevuti via email o chat: potrebbero essere tentativi di phishing per rubare le tue credenziali.
- Non scaricare o installare software non autorizzato.
- Non collegare chiavette USB personali senza l'autorizzazione del docente.

4.3 Prima di lasciare il PC — Checklist di uscita

✓ Fai SEMPRE questi 4 passaggi prima di alzarti

1. Esci da Gmail e da tutti i servizi Google (clicca sulla tua iniziale in alto a destra → “Esci”).
2. Esci da qualsiasi altro sito su cui ti sei autenticato.
3. Chiudi TUTTE le finestre del browser.
4. Se possibile, cancella i dati di navigazione (Ctrl+Shift+Canc → seleziona tutto → Cancella dati).

Ricorda: anche chiudere il browser senza fare logout NON è sufficiente. La sessione Google resta attiva e chiunque apra il browser dopo di te avrà accesso alla tua posta, ai tuoi file e ai tuoi voti su Classroom.

5. I rischi concreti: cosa può succedere

Le seguenti situazioni si sono già verificate in contesti scolastici e possono avere conseguenze gravi:

Rischio	Scenario	Conseguenze
Sessione lasciata aperta	Uno studente dimentica di fare logout da Gmail su un PC di laboratorio. Un compagno legge la sua posta, invia messaggi a suo nome o accede ai suoi file.	Provvedimento disciplinare per entrambi. Possibile denuncia penale per accesso abusivo (art. 615-ter c.p.).
Password condivisa	Due amici si scambiano la password “per comodità”. Dopo un litigio, uno dei due usa l’account dell’altro per inviare messaggi offensivi ai docenti.	Responsabilità del titolare dell’account. Procedimento disciplinare e potenziale segnalazione alle autorità.
Password salvata nel browser	Lo studente clicca “Ricorda password” su Chrome. Chiunque acceda a quel PC può entrare nel suo account senza conoscere la password.	Accesso non autorizzato ai dati personali, alla posta e ai compiti.
Phishing	Lo studente riceve una mail che sembra provenire da Google e inserisce le proprie credenziali su un sito falso.	Furto di credenziali, accesso fraudolento all’account, possibile compromissione dei dati di tutto il dominio scolastico.
Uso improprio dell’account	Lo studente usa l’account scolastico per registrarsi a servizi non didattici, esponendo l’indirizzo a spam e potenziali violazioni.	Possibile blocco dell’account. Richiamo formale.

6. Cosa dice la legge

L’accesso non autorizzato a un account informatico altrui è un reato penale in Italia, anche se l’account è stato lasciato aperto e anche se non si arreca un danno evidente.

6.1 Art. 615-ter del Codice Penale

«Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione da uno a cinque anni.»

Questo significa che: anche se trovi un account aperto su un PC di laboratorio, non sei autorizzato ad usarlo. Il fatto che la “porta fosse aperta” non è una giustificazione legale. Leggere la posta altrui, inviare messaggi o anche solo “curiare” costituisce reato.

6.2 Responsabilità del titolare dell’account

Chi lascia la propria sessione aperta su un PC condiviso commette una negligenza. Pur non essendo direttamente responsabile delle azioni compiute da terzi, il titolare può essere soggetto a provvedimenti disciplinari interni per mancata custodia delle credenziali.

6.3 Tracciabilità

Ogni azione compiuta con un account Google Workspace è registrata nei log di sistema della Google Admin Console. L’amministratore del dominio scolastico può risalire a: data e ora di ogni accesso, indirizzo IP di origine, tipo di dispositivo utilizzato, messaggi inviati e ricevuti, file consultati e modificati. I log sono conservati per un periodo minimo di 6 mesi e possono essere utilizzati in sede disciplinare e giudiziaria.

7. La verifica in due passaggi (2FA)

La verifica in due passaggi aggiunge un secondo livello di protezione: oltre alla password, dovrai confermare l’accesso tramite il tuo smartphone. Anche se qualcuno scopre la tua password, non potrà entrare nel tuo account senza il tuo telefono.

7.1 Come attivarla

1. Vai su myaccount.google.com con il tuo account scolastico.
2. Clicca su “Sicurezza” nel menu a sinistra.
3. Nella sezione “Accesso a Google”, clicca su “Verifica in due passaggi”.
4. Segui la procedura guidata: ti verrà chiesto di associare il tuo numero di telefono.
5. Scegli il metodo preferito: notifica push su Google (consigliato), SMS, o app di autenticazione (Google Authenticator).

L’attivazione della 2FA è fortemente consigliata per tutti e potrebbe diventare obbligatoria.

8. Indicazioni specifiche per i docenti

- All’inizio di ogni sessione di laboratorio, ricordare agli studenti di effettuare il logout al termine.
- Al termine della lezione, verificare che tutti abbiano effettuato il logout prima di lasciare il laboratorio.
- Non lasciare il proprio account aperto sui PC del laboratorio o dell’aula docenti.
- Segnalare tempestivamente agli amministratori qualsiasi sospetto di accesso non autorizzato.

- Non condividere le proprie credenziali con colleghi o studenti, nemmeno temporaneamente.

9. Cosa fare se...

9.1 ...trovi un account altrui aperto su un PC

1. NON utilizzare l'account e NON leggere i contenuti.
2. Fai il logout dall'account (clicca sull'iniziale in alto a destra → "Esci").
3. Avvisa il docente presente in laboratorio.
4. Se possibile, avvisa anche il compagno proprietario dell'account affinché cambi la password.

9.2 ...sospetti che qualcuno abbia usato il tuo account

- Cambia immediatamente la password.
- Controlla l'attività recente in myaccount.google.com → Sicurezza.
- Verifica la posta inviata: qualcuno potrebbe aver spedito messaggi a tuo nome.
- Controlla i filtri e le regole di inoltro in Gmail: un intruso potrebbe aver impostato un inoltro automatico.
- Avvisa il docente e gli amministratori.

9.3 ...ricevi una mail sospetta che ti chiede le credenziali

- NON cliccare su nessun link contenuto nella mail.
- Google non chiede MAI la tua password via email.
- Segnala la mail come phishing (in Gmail: tre puntini → "Segnala phishing").
- Avvisa il docente e gli amministratori.

10. Le 10 regole d'oro

1	La tua password è solo TUA. Non condividerla mai con nessuno.
2	Fai sempre LOGOUT quando finisci di usare un PC condiviso.
3	Su PC di laboratorio, usa la navigazione in incognito (Ctrl+Shift+N).
4	Non selezionare mai "Ricorda password" su PC non tuoi.
5	Se trovi un account altrui aperto, NON usarlo. Fai logout e avvisa un docente.
6	Attiva la verifica in due passaggi (2FA) sul tuo account.
7	Cambia la password almeno una volta a quadrimestre.
8	Non aprire link sospetti e non inserire mai le credenziali su siti non ufficiali.
9	Se sospetti un accesso non autorizzato, cambia la password e avvisa subito.
10	Ricorda: ogni azione con il tuo account è tracciata e riconducibile a te.

Il presente vademecum viene distribuito a tutti gli studenti e al personale dell'istituto. La presa visione e l'accettazione delle regole in esso contenute è condizione necessaria per l'utilizzo dell'account scolastico e dei PC di laboratorio.

Il Referente ICT / Animatore Digitale

Visto: Il Dirigente Scolastico
