REGOLAMENTO
SISTEMI INFORMATICI
- STUDENTI -

REGOLAMENTO INTERNO
SISTEMI INFORMATICI

INDICE

CAPO I – I PRINCIPI

ART. 1 INTRODUZIONE, DEFINIZIONI E FINALITÀ

Il presente disciplinare interno ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo dei sistemi informatici dell'istituto da parte degli utenti (studenti) al fine di tutelare i beni dell'Istituto ed evitare condotte che potrebbero esporre l'Istituto a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.
L'insieme delle norme comportamentali qui incluse, pertanto, è volto a conformare l'Istituto ai principi di diligenza, informazione e correttezza anche sulla base della vigente normativa nazionale, con particolare riferimento al *Regolamento UE 2016/679 e successiva regolamentazione D. Lgs. 101/2018*, ed ai provvedimenti appositamente emanati dall'Autorità Garante.

ART. 2 AMBITO DI APPLICAZIONE

Il presente disciplinare interno si applica ad ogni *Utente,* studente/studentessa, che utilizza servizi e risorse informative di pertinenza dell'Istituto.

Per *Utente* si intende ogni studente/studentessa che utilizza beni e servizi informatici all'interno della struttura scolastica.

Con *Istituto* si intende il Liceo Scientifico "Niccolò Copernico", scuola titolare dei beni e delle risorse informatiche ivi disciplinate, nonché Titolare del trattamento dei dati.

Con *sistemi informatici*, in questo disciplinare si intendono:

- i dispositivi informatici dell'istituto (computer, stampanti,...) e i software installati su questi messi a disposizione
- la connettività internet tramite la rete dell'istituto
- i servizi ICT, ovvero i processi e le pratiche connesse alla trasmissione, ricezione ed elaborazione dei dati e delle informazioni; tra questi servizi figurano: la posta elettronica, i servizi cloud e comunque qualunque sistema informatico/procedura attraverso cui vengano trattati dati personali in connessione con l'attività lavorativa

ART. 3 TITOLARITÀ DEI BENI E DELLE RISORSE INFORMATICHE

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni di esclusiva proprietà dell'Istituto. Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni e compiti affidati ad ogni Utente per scopi riguardanti l'attività didattica, e comunque per l'esclusivo perseguimento delle finalità istituzionali e nelle modalità previste dal Titolare.

ART. 4 RESPONSABILITÀ PERSONALE DELL'UTENTE

Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'Istituto.
Con l'obiettivo di preservare l'integrità dei beni e delle risorse dell'Istituto, ogni Utente è tenuto a:

- tutelare i beni dell'Istituto da utilizzi impropri e non autorizzati;
- ad operare, in relazioni al proprio ruolo e alle mansioni in concreto svolte, a tutela della sicurezza informatica, riportando al Dirigente scolastico e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente disciplinare interno;
- non mettere in atto comportamenti che possano creare un danno, anche d'immagine, all'Istituto;
- rispettare quanto previsto dagli specifici Regolamenti di Istituto (regolamenti laboratori, regolamenti attrezzature d'aula,…).

Per ragioni organizzative ovvero per esigenze dettate dalla sicurezza del lavoro ovvero per la tutela del patrimonio, i sistemi informatici, gli impianti, le apparecchiature o i dispositivi saranno sottoposti a monitoraggi e controlli di funzionamento periodici, anche da piattaforme che agiscono a distanza.
Le operazioni di monitoraggio saranno effettuate dagli amministratori di sistema, come indicato nell'Art. 5.
Fermo restando il diritto dell'Istituto di effettuare tali controlli, essi saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei cittadini, nel rispetto del principio di pertinenza e non eccedenza, non saranno costanti, prolungati e indiscriminati.

CAPO II – MISURE ORGANIZZATIVE

ART. 5 AMMINISTRATORI DEI SISTEMI INFORMATICI

L'Istituto conferisce agli amministratori di sistema il compito di sovrintendere ai beni e alle risorse informatiche scolastiche. In particolare, sulla base di una divisione delle competenze, sono individuati due amministratori:

- **amministratore di sistema dell'area amministrativa** da qui in seguito indicato con **ASAA** (area comprendente i server dedicati al controller di dominio, dispositivi di backup in rete, PC destinati al personale amministrativo, al DSGA, al Dirigente scolastico): **Raffaele Pilosio (Integra Sistemi Srl)**

- **amministratore di sistema dell'area didattica e infrastruttura di rete** da qui in seguito indicata con **ASAD** (area comprendente tutti gli asset e apparati informatici non inclusi nell'area amministrativa): **Fabio Maria Antoniali (docente interno)**

Sulla base delle specifiche aree di competenza, è compito di ciascun amministratore di sistema, avvalendosi anche della collaborazione del personale tecnico dell'Istituto:

- gestire, con la collaborazione degli Assistenti Tecnici, l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'Istituto;
- gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
- monitorare il corretto utilizzo delle risorse di rete, dei server, dei personal computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati, tutela del patrimonio;
- creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
- provvedere alla sicurezza informatica dei sistemi informativi, nel rispetto di quanto prescritto dal *D. Lgs 196/2003*, dal *Regolamento UE 2016/679 e successiva regolamentazione D. Lgs. 101/2018*;
- utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un Utente in caso di prolungata assenza, irreperibilità o impedimento dello stesso.

ART. 6 AMMINISTRATORI DEI SERVIZI ITC

Accanto agli amministratori di sistema, l'Istituto conferisce ad alcuni utenti il compito di sovrintendere all'amministrazione di alcuni specifici servizi ITC (Tecnologie dell'Informazione e della Comunicazione) a cui accede l'utenza.
Qui di seguito vengono riportati gli amministratori che, sulla base di una divisione di competenze, incaricati di intervenire sulla creazione, configurazione, aggiornamento, sospensione, cancellazione monitoraggio degli account degli Utenti.

Servizi Spaggiari	
Nome	**Ruolo**
Braida Michela (docente interno)	Creazione e modifica account degli studenti/studentesse
Assistenti amministrativi dell'ufficio alunni	Sospensione e cancellazione account degli studenti/studentesse e dei relativi

	dati personali

Google Workspace	
Nome	**Ruolo**
Sambo Cristina (docente interno)	Creazione, configurazione, modifica, sospensione e cancellazione degli account e dei dati del personale esterno, creazione, configurazione e cancellazione dei gruppi non standard. Rigenerazione credenziali di accesso. Monitoraggio degli accessi degli utenti al GW e alle sue app, monitoraggio, definizione delle liste delle app di terze parti autorizzate / non autorizzate ad accedere ai dati del GW.
Andretta Andrea (docente interno)	Creazione, configurazione, modifica, sospensione e cancellazione degli account e dei dati del personale esterno, creazione, configurazione e cancellazione dei gruppi non standard. Rigenerazione credenziali di accesso. Monitoraggio degli accessi degli utenti al GW e alle sue app, monitoraggio, definizione delle liste delle app di terze parti autorizzate / non autorizzate ad accedere ai dati del GW.
Antoniali Fabio Maria (docente interno)	Creazione, configurazione, modifica, sospensione e cancellazione degli account del personale scolastico e degli studenti e dei loro dati, creazione, configurazione, aggiornamento, cancellazione dei gruppi ordinari. Rigenerazione credenziali di accesso. Monitoraggio degli accessi degli utenti al GW e alle sue app, monitoraggio, definizione delle liste delle app di terze parti autorizzate / non autorizzate ad accedere ai dati del GW.

Sito web istituzionale	
Nome	**Ruolo**

Antoniali Fabio Maria (docente interno)	Creazione, modifica, profilazione, cancellazione degli account che accedono al backend del sito web

Piattaforme Servizi Web e Copernicorsi	
Nome	**Ruolo**
Antoniali Fabio Maria (docente interno)	Profilazione, modifica e cancellazione degli account e dei dati del personale scolastico e, relativamente a Copernicorsi, dell'utenza (famiglie e studenti)

Moodle	
Nome	**Ruolo**
Antoniali Fabio Maria (docente interno)	Profilazione, modifica, configurazione e cancellazione degli account e dei dati del personale scolastico e all'utenza
Mosangini Matteo (docente interno)	Profilazione, modifica, configurazione e cancellazione degli account e dei dati del personale scolastico e all'utenza

ART. 7 ACCOUNT SERVIZI SPAGGIARI

1. I principi

Agli studenti/studentesse viene fornito un account per l'accesso ai **Servizi Spaggiari**, in particolare alle piattaforme ClasseViva, con funzioni di registro elettronico, e Scuola & Territorio, per la gestione dei PCTO.

2. Creazione e gestione degli Account

Un account Utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche scolastiche.

Gli account sono associati univocamente alla persona assegnataria e vengono creati dall'amministratore dei Servizi Spaggiari;

1. l'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione" (es. "Username/Email" e "Password"), comunicate all'Utente attraverso modalità che ne garantiscano la segretezza;
2. non è consentito comunicare le proprie credenziali di autenticazione a terzi,

anche se soggetti in posizione apicale all'interno dell'Istituto;
3. se l'Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password e a segnalare la violazione all'amministratore del sistema nonché al Dirigente scolastico, in veste di Responsabile della protezione dei dati;
4. ogni Utente è responsabile dell'utilizzo del proprio account utente.

3. Protezione account e password di accesso

Dal primo accesso con le credenziali di autenticazione, l'Utente è invitato a cambiare periodicamente le credenziali e, nel definire la password, a rispettare le regole riportate **nell'Allegato A** del presente regolamento.
Come misura di sicurezza, si consiglia di non salvare nel browser le credenziali in dispositivi di uso non esclusivo.
Si ricorda che scrivere la password su post-it o altri supporti, nonché memorizzarla in chiaro in forma digitale, costituisce violazione del presente regolamento.

4. Cessazione degli Account

Alla conclusione del percorso di studi o in caso di ritiro dell'Utente, le credenziali di autenticazione di cui sopra verranno immediatamente **disabilitate**.

ART. 8 ACCOUNT DI ACCESSO AI SERVIZI ONLINE

1. I principi

All'Utente viene concesso un account per l'accesso alla piattaforma **Google Workspace,** d'ora in poi indicata con **GW**, con username creato secondo lo schema **cognome.nome@liceocopernico.org**. L'accesso è subordinato all'accettazione da parte dell'Utente e dei genitori/tutori (in caso di utente minorenne) delle regole di utilizzo consegnate all'atto dell'iscrizione all'Istituto.
L'Istituto utilizza server Google per l'erogazione del servizio, su tali server ogni utente avrà a disposizione una casella di posta elettronica, l'accesso ai servizi principali della piattaforma Google e ai servizi aggiuntivi.
Le applicazioni a disposizione dell'utente, fruibili via internet, sono attivabili o meno a discrezione dell'Istituto, che ne definisce di volta in volta regole e limiti di utilizzo, in base alle esigenze legate all'attività svolta, indipendentemente dalle possibilità tecniche offerte dalla piattaforma di Google.

Mediante l'account **GW** gli Utenti possono accedere, inoltre, ai seguenti servizi gestiti dall'Istituto:
- piattaforma Copernicorsi (per la registrazione alle attività di recupero e sportello)
- ai pc dei laboratori e delle classi

2. Creazione e gestione degli Account

Un account Utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche scolastiche.

1. L’account GW viene creato all’iscrizione dell’Utente presso l’Istituto, e rimane attivo per tutto il percorso degli studi presso l’Istituto;
2. gli account utenti sono associati univocamente alla persona assegnataria e vengono creati dagli amministratori di Google Workspace (vedasi Art. 6)**;**
3. l’accesso al proprio account avviene tramite l’utilizzo delle “credenziali di autenticazione” (es. “Username/Email” e “Password”), comunicate all’Utente attraverso modalità che ne garantiscano la segretezza (Es: comunicazione tramite bacheca del registro elettronico, one-time password, link, comunicazione tramite ufficio alunni);
4. le credenziali di autenticazione sono strettamente personali, pertanto non possono essere comunicate ad altre persone;
5. se l’Utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, lo stesso è tenuto a modificare immediatamente la password e/o a segnalare la violazione all’amministratore del sistema nonché al Dirigente scolastico, in veste di Responsabile della protezione dei dati;
6. ogni Utente è responsabile dell’utilizzo del proprio account utente.

3. Protezione account e password di accesso

La password di accesso viene fornita all’Utente con una modalità che ne garantisca la riservatezza e, per impostazione di sistema, deve essere modificata contestualmente al primo accesso.
Per gli utenti del GW è configurata una *policy* che impone la sostituzione periodica della password**;** la stessa *policy* determina la scadenza della sessione di login ogni **24 ore**.
L'Utente nel definire la password è invitato a seguire le regole riportate nell’**Allegato A** del presente regolamento.
Come misura di sicurezza, si consiglia di non salvare nel browser le credenziali in dispositivi di uso non esclusivo.
Si ricorda che scrivere la password su post-it o altri supporti, nonché memorizzarla in chiaro in forma digitale, costituisce violazione del presente regolamento.

4. Accesso ai Servizi Google aggiuntivi

Sulla base di motivate esigenze didattiche, sentito anche il parere del DPO in materia di tutela dei dati e con l’autorizzazione del Dirigente scolastico, gli AGW possono consentire a particolari categorie di utenti l’accesso ai *Servizi Google aggiuntivi.* La lista dei servizi aggiuntivi attivati è riportata nell’Allegato C.

5. Accesso di app e servizi di terze parti ai dati del workspace

Tramite ***Accedi con Google*** è possibile accedere ad app e servizi di terze parti, creando un’esperienza di registrazione e *sign in* semplificata. Questo meccanismo prevede la condivisione con questi servizi ed app delle informazioni del proprio profilo, ovvero: **nome**, **indirizzo email**, **immagine del profilo** (di qui in poi indicati come *informazioni profilo*).

L’utilizzo da parte dell’utente di una app che accede alle sole informazioni profilo dell’account istituzionale è consentito purché:

- la app sia strettamente attinente all'attività didattica;
- la app non richieda la sottoscrizione di un contratto che preveda la registrazione di mezzi di pagamento di qualunque genere associati ad una persona fisica.

Alcuni di questi servizi e app potrebbero però richiedere all'utente di concedere autorizzazioni per accedere anche ad altri dati, ad esempio alla posta elettronica, alle foto, ai documenti del drive, ai dati dei corsi di classroom eccetera. Concedere l'accesso a questi dati potrebbe costituire un trattamento illecito dei dati ed essere in conflitto con il Regolamento Privacy (GDPR). A titolo esemplificativo, una app a cui è stato concesso l'accesso in lettura e scrittura al drive, ha la capacità di accedere, modificare ed eliminare tutti i documenti di proprietà dell'utente o che sono stati condivisi da altri con l'utente.

Come misura di rafforzamento della tutela dei dati personali, la piattaforma è configurata in modo da bloccare automaticamente l'accesso di app e servizi che, oltre alle informazioni del profilo utente, accedono ad altri dati del GW (Persone, Drive, GMail, Classroom...). Per ridurre i rischi **l'accesso è consentito solo per le app e servizi della *white list* riportata nell'Allegato C**.

6. Modifiche alla *white list* delle app di terze parti autorizzate

Gli **AGW** effettuano periodici monitoraggi delle app di terze parti e **potranno in qualunque momento e senza alcun preavviso disconnettere l'accesso degli utenti ad applicazioni e servizi di terze parti non presenti nella *white list*, ed eventualmente bloccare del tutto l'accesso dell'app/servizio ai dati del Workspace.**

Nel caso in cui emergessero rischi per la sicurezza o per la tutela della privacy relativi ad una delle app presenti nella *white list*, il Dirigente scolastico si riserva la possibilità di sospendere l'autorizzazione al suo utilizzo, in attesa di accertamenti. In tal caso, gli AGW daranno agli utenti un preavviso di almeno **10 giorni** tramite la mail istituzionale, quindi, trascorso tale periodo, configureranno la piattaforma in modo da bloccare l'accesso dell'app ai dati del workspace.

L'Istituto non sarà responsabile verso gli utenti, nonché verso soggetti direttamente o indirettamente loro connessi, e verso i terzi per i danni, le perdite di profitti e i costi sopportati in conseguenza del blocco dell'accesso di un app o servizio di terze parti ai dati del workspace istituzionale.

Considerati i rischi incombenti sulla protezione dei dati, è opportuno che ciascun utente **controlli periodicamente quali servizi accedono ai dati del GW** e quali dati sono coinvolti, eventualmente rimuovendo le autorizzazioni precedentemente concesse. Maggiori dettagli sulla **gestione dei servizi e app di terze** parti sono disponibili alla pagina:
https://support.google.com/accounts/answer/3466521?hl=it&ref_topic=7188760

7. Compiti degli Amministratori

Nella gestione della piattaforma, gli AGW si impegneranno ad operare rispettando la privacy degli Utenti, richiedendo solo le informazioni strettamente necessarie per permettere l'accesso al Servizio ed impegnandosi a non divulgare in alcun modo. Si precisa in particolare che tramite la Console di amministrazione della GW gli AGW:

- possono visualizzare i profili utente e la struttura organizzativa;
- possono gestire le singole impostazioni di sicurezza di un utente (p. es. monitorare il livello di sicurezza delle password, gestire la verifica in due passaggi)
- possono eseguire ricerche relative agli eventi del log Utente, per verificare le azioni critiche eseguite dagli Utenti nei propri account. Queste azioni includono modifiche di password non autorizzate dall'utente, dettagli per il recupero dell'account (numeri di telefono, indirizzi email), e se un utente accede da un client di posta o da un'applicazione diversa dal browser, possono anche esaminare i rapporti sui tentativi di accesso sospetti;
- possono modificare le credenziali di accesso di un Utente solo su richiesta esplicita dell'Utente stesso (ad esempio se l'Utente non riesce più ad accedere al proprio Account);
- non sono in possesso delle password di accesso al sistema dei singoli Utenti (potranno solo cambiarle, su loro richiesta);
- possono visualizzare log e statistiche sull'utilizzo del sistema (ad esempio: data dell'ultimo accesso o spazio utilizzato).

8. Azioni specifiche sui dispositivi mobili

Gli AGW, allo scopo di garantire la sicurezza dei dati del workspace, possono svolgere le seguenti azioni sull'account degli utenti:

1. Personalizzare i requisiti relativi alle password per i dispositivi mobili gestiti per assicurare che vengano soddisfatti i criteri di sicurezza per l'accesso agli account
2. Configurare le app gestite per i dispositivi Android allo scopo di mettere a disposizione degli utenti le applicazioni di uso comune per la didattica e di impostare le configurazioni più idonee per le attività svolte
3. Cancella i dati dell'account istituzionale di un utente da un dispositivo mobile in caso di smarrimento o furto del dispositivo per ridurre il rischio di data breach .
4. Configurare gli avvisi di attività per i dispositivi mobili in modo da fornire notifiche su attività specifiche che si verificano nel dominio, ad esempio un tentativo di accesso sospetto, un dispositivo mobile compromesso o la modifica delle impostazioni da parte di un altro amministratore.
5. Periodicamente, esaminare i dispositivi mobili che accedono ai dati dell'organizzazione, ad esempio per valutare l'utilizzo dei dispositivi assegnati in comodato d'uso o individuare dispositivi che presentano rischi sotto il profilo della sicurezza (sistemi non aggiornati, stato "rooted" o "jailbroken", …).

9. Cessazione degli Account

Alla conclusione del ciclo di studi, sarà cura dell'Utente recuperare i propri dati e documenti personali entro il **31 luglio**. L'account e tutti i dati associati saranno **definitivamente eliminati** entro il **31 agosto**.

In caso di richiesta di ritiro o di trasferimento in altra scuola, lo studente avrà cura di recuperare i propri dati e documenti personali entro la data di espletamento della suddetta procedura amministrativa. L'account e i dati associati verranno eliminati entro **15 giorni**.

Si precisa che per tutela della privacy la funzionalità *Takeout* - funzionalità che consente di migrare i dati tra diversi account GW - non è abilitata, pertanto gli utenti che intendono conservare email o documenti personali presenti nel workspace dovranno provvedere al backup dei dati con altri strumenti.

CAPO III – CRITERI DI UTILIZZO DEI SISTEMI INFORMATICI DELL'ISTITUTO

ART. 9 POSTAZIONI DI LAVORO

L'Utente che utilizza i computer dell'Istituto e relative periferiche è tenuto a rispettare i regolamenti dedicati:

- regolamenti dei laboratori di informatica, fisica e scienze
- regolamento delle attrezzature d'aula

CAPO IV– CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI PERSONALI (BYOD)

ART. 10 USO DI DEVICE PERSONALI

1. Definizione dell'approccio BYOD

La tecnologia, se utilizzata in modo responsabile e corretto, fornisce agli studenti opportunità innovative per incrementare la loro cultura, in linea con quanto specificato nell'azione #6 del Piano Nazionale Scuola Digitale (PNSD) "Politiche attive per il BYOD" (*Bring Your Own Device,* ovvero porta un tuo dispositivo).
Il nostro Istituto vuole favorire tale processo garantendone la sicurezza attraverso una modalità di interazione che contribuisca al miglioramento dell'ambiente educativo e di apprendimento e mira a garantire a tutti gli studenti una formazione digitale che parta dal saper usare i propri dispositivi in maniera consapevole e adeguata.
Vengono pertanto definiti un insieme di criteri che consentono agli Utenti di utilizzare i propri dispositivi (telefono, laptop, tablet o altro) per accedere alle applicazioni e ai dati che concernono l'attività didattica.

2. Accesso alla rete di istituto

Non è consentito, di norma, a studenti/studentesse l'accesso alla rete Wi-Fi di Istituto o alla rete cablata.

3. Utilizzo dei dispositivi all'interno dell'istituto

- Come dispositivi personali sono ammessi a scuola: computer portatile, tablet, e-reader, cellulari.
- Non è ammesso l'uso a scuola di console di gioco, né di qualunque tipo di videogioco.
- I dispositivi devono essere usati a scuola per soli scopi didattici e solo con l'autorizzazione dell'insegnante. Agli studenti/studentesse non è permesso usare dispositivi elettronici per giochi durante le ore scolastiche.
- E' vietato agli studenti/studentesse usare dispositivi di registrazione audio, videocamere o fotocamere per registrare video o fare foto in classe senza il permesso dell'insegnante e senza il consenso della persona che viene registrata o ripresa; in ogni caso, tali registrazioni o immagini sono per uso strettamente personale e non possono essere diffuse o trasmesse ad altri tramite instant messaging, social network, siti internet, ecc..
- Eventuali audio e video registrati a scuola a fini didattici sono sotto la responsabilità e la stretta sorveglianza degli insegnanti.
- Agli studenti/studentesse non è permesso usare i propri dispositivi al di fuori dell'orario di lezione come ad esempio pause, uscite didattiche, visite guidate, viaggi d'istruzione, attività facoltative extracurricolari, manifestazioni sportive, spettacoli teatrali ecc., esclusa la ricreazione, se non con l'esplicita autorizzazione del docente responsabile della classe.
- Gli studenti/studentesse sono responsabili personalmente dei dispositivi portati a scuola e devono custodirli con cura e attenzione. La scuola non risponde di eventuali furti o smarrimenti.
- E' in capo agli studenti/studentesse la responsabilità di riportare a casa il dispositivo al termine delle lezioni. L'Istituto non assume la responsabilità per la custodia di nessun dispositivo degli studenti/studentesse lasciato a scuola e non è responsabile della custodia dei dispositivi e di eventuali danni ad essi cagionati dal proprietario o da altri studenti/studentesse.
- Agli studenti/studentesse è richiesto di caricare completamente il proprio dispositivo a casa: non sarà possibile ricaricarlo durante l'orario di lezione. Si consiglia di dotarsi di batterie portatili.

Per un uso corretto e appropriato dei BYOD, agli studenti è vietato:

- usare Internet per scopi diversi da quelli didattici;
- scaricare musica, video e programmi da Internet o qualsiasi file senza il consenso dell'insegnante;
- utilizzare i social network per fini diversi da quelli didattici e senza la supervisione del docente;
- giocare sul computer, in rete o offline (a meno che il gioco non faccia parte di una lezione e sia supervisionato dall'insegnante);
- utilizzare la Rete e i social network per deridere, offendere, denigrare compagni, docenti, personale scolastico, parenti/amici dei compagni sia in orario scolastico sia in orario extrascolastico; si ricorda che il cyberbullismo è un reato e qualsiasi atto degli studenti che dovesse configurarsi come reato verrà denunciato d'ufficio alle forze dell'ordine. Alla denuncia d'ufficio può sommarsi la querela da parte della persona chiamata in causa.

4. Accesso ai dati del Google Workspace sui dispositivi fissi e laptop

Nell'utilizzo di applicazioni che accedono ai dati del workspace (applicazioni web fruite tramite il browser, client email, sistemi di sincronizzazione,...) si raccomanda di adottare le seguenti misure:

- utilizzare solo PC in cui sistema operativo e le applicazioni sono mantenute regolarmente aggiornate, in cui è presente un software antimalware
- evitare l'utilizzo di dispositivi di cui non si ha un controllo esclusivo, cioè amministrati dall'Utente o dai propri genitori/tutori
- durante l'attività non connettersi a reti wifi di accesso pubblico (ad esempio quelle messe a disposizione da ristoratori, strutture turistiche ricettive, comuni, ospedali...), a meno di non proteggersi utilizzando una VPN che garantisca sicurezza e privacy delle connessioni
- se si è installato il programma *Backup e sincronizzazione o Drive for desktop* che sincronizza il Drive istituzionale in una cartella locale del dispositivo, al fine di tutelare i dati nel caso di furto/smarrimento o tentativo di accesso da parte di terzi, è consigliata la crittografia della memoria di massa del dispositivo (ad esempio attivando la crittografia Bitlocker nei sistemi con SO Windows che lo supportano)
- l'Utente si impegna ad adottare le necessarie e dovute cautele per assicurare la segretezza delle credenziali di accesso al dispositivo, se c'è il sospetto che un soggetto non autorizzato ne sia venuto a conoscenza, dovrà provvedere immediatamente a cambiarla
- In caso di furto o smarrimento del dispositivo, o in qualunque altro caso in cui l'Utente sospetta che il controllo del dispositivo sia stato compromesso (ad esempio a causa di un sospetto malware o per un accesso non autorizzato) è tenuto a:
    - effettuare la disconnessione remota dell'account GW istituzionale dal device dal pannello *Account > Sicurezza > I tuoi dispositivi*
    - cambiare immediatamente la password dell'account GW
    - cambiare immediatamente la password dell'account dei Servizi Spaggiari
    - dare immediata segnalazione all'Istituto dell'accaduto per attivare una valutazione dell'incidente e verificare se sussiste la possibilità di un *data breach*

5. Accesso ai dati del Google Workspace sui dispositivi mobili

L'accesso ai dati del workspace con i dispositivi mobili (tablet e smartphone), per loro natura maggiormente soggetti a furto o smarrimento, aumenta significativamente i rischi relativi alla sicurezza e protezione dei dati. Pertanto si raccomanda all'utente di adottare le seguenti misure:

- connettersi a reti wifi di accesso pubblico (ad esempio quelle messe a disposizione da ristoratori, strutture turistiche ricettive, comuni, ospedali...) solo utilizzando una VPN che garantisca sicurezza e privacy delle connessioni;
- adottare un meccanismo di **blocco schermo** basato su uno dei seguenti sistemi: PIN (min 5 cifre numeriche), password o sistema biometrico, che ne

impedisca l'utilizzo da parte di soggetti non autorizzati;

- adottare le necessarie e dovute cautele per assicurare la segretezza delle credenziali di accesso al dispositivo; se c'è il sospetto che un soggetto non autorizzato sia venuto a conoscenza della password, dovrà provvedere immediatamente a cambiarla;
- in caso di furto o smarrimento del dispositivo, o in qualunque altro caso in cui l'Utente sospetta che il controllo del dispositivo sia stato compromesso (ad esempio a causa di un sospetto malware o per un accesso non autorizzato) dovrà:
    - effettuare la disconnessione remota dell'account GW istituzionale dal device dal pannello *Account* > *Sicurezza* > *I tuoi dispositivi*
    - cambiare immediatamente la password dell'account GW
    - cambiare immediatamente la password dell'account RE
    - dare immediata segnalazione all'Istituto dell'accaduto per attivare un valutazione dell'incidente e verificare se sussistono le condizioni di un data breach

6. Norme ulteriori per i dispositivi mobili Android o iOS

Nel momento in cui un utente aggiunge l'account GW su un dispositivo mobile personale di tipo Android o iOS, deve tenere presente che l'amministrazione potrà intervenire, in modo più o meno esteso, su tale dispositivo e sui dati in esso presenti. L'entità dell'intervento consentito all'amministrazione dipende dalla modalità con cui è configurato l'account GW.
Per studenti/studentesse è attiva per impostazione predefinita la **gestione di base**, la quale consente agli amministratori di impostare requisiti di base relativi ai passcode, gestire le app (solo Android) e ricevere informazioni dettagliate (p. es. nome del dispositivo, sistema operativo, ultima sincronizzazione) sui dispositivi su cui sono configurati account istituzionali.

7. Dispositivi di memoria rimovibili

Per dispositivi di memoria rimovibili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati esternamente al computer. Sono considerati tali CD-ROM, DVD, memorie USB, card digitali, dischi rigidi esterni.

Sebbene i supporti rimovibili siano utili per l'archiviazione e il trasferimento dei dati, comportano alcuni rischi alla sicurezza dei dati. Ogni volta che si copiano dati su supporti rimovibili, c'è il rischio che i dati siano accessibili e intercettati da entità non autorizzate. Inoltre, poiché sono piccoli e facili da trasportare, le probabilità che vengano persi o rubati sono elevate.
Si invitano quindi gli Utenti che utilizzano tali dispositivi a non conservare in essi dati personali. Si precisa che, una volta connesso un dispositivo di memoria ad un PC dell'Istituto, i dati contenuti in questi dispositivi vengono considerati alla stregua di file scaricati tramite la connettività internet dell'istituto e sono pertanto soggetti (ove previsto) al presente disciplinare interno e regolamenti citati nell'art. 9.

8. Altri dispositivi rimovibili

Gli apparecchi di proprietà personale dell'Utente non rientranti nelle categorie del punto 1 del presente articolo (telefoni cellulari, lettori musicali o di altro tipo, fotocamere digitali, ecc.) non potranno essere collegati ai computer o alle reti informatiche scolastiche, salvo nel caso in cui sia stata concessa espressa autorizzazione da parte del Dirigente scolastico.

CAPO V – GESTIONE DELLE COMUNICAZIONI TELEMATICHE

ART. 11 GESTIONE UTILIZZO DELLA RETE

1. Norme generali sull'utilizzo della connettività internet

E' sconsigliato connettersi a reti wifi o cablate di accesso pubblico (ad esempio quelle messe a disposizione da ristoratori, strutture turistiche ricettive, comuni, ospedali...), a meno di non proteggersi utilizzando una VPN che garantisca sicurezza e privacy delle connessioni.

Riguardo l'uso della applicazioni disponibili sulla rete internet

- Non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'Istituto in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente dal Dirigente scolastico;
- Eventuali commenti lesivi dell'immagine dell'istituto pubblicati in rete potranno essere oggetto di sanzioni disciplinari e, dove ricorrano gli estremi, di denuncia all'autorità giudiziaria

2. Norme specifiche sull'utilizzo della connettività internet istituzionale

Col presente disciplinare interno si richiama gli utenti ad una particolare attenzione nell'utilizzo della rete istituzionale (**RI)** e dei servizi relativi, in quanto ogni operazione posta in essere è associata all'indirizzo Internet Pubblico assegnato all'Istituto.
La **RI** è uno strumento messo a disposizione degli utenti per uso didattico. Ciascun Utente, pertanto, deve usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve quindi prendere ogni precauzione a tale riguardo.

Sulla RI **non sono consentite** le seguenti attività:

A. Violare la sicurezza di archivi e computers della rete o la privacy di altri utenti connessi ad internet; compromettere il funzionamento della LAN dell'istituto o di internet, nonché delle apparecchiature che le costituiscono o degli host ad esse collegati con programmi (virus, trojan horses, ecc.) costruiti appositamente; si precisa che queste attività costituiscono dei veri e propri crimini e pertanto sono punibili dalla legge.

B. L’effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dal Dirigente scolastico.
C. La partecipazione a forum, l’utilizzo di chat-line o di bacheche elettroniche e le registrazioni in *guest-book*, anche utilizzando pseudonimi (o nicknames), salvo casi espressamente autorizzati dal Dirigente scolastico.
D. La navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
E. L’utilizzo di soluzioni di instant messenger e/o chat se non per scopi didattici ed attraverso gli strumenti ed i software messi a disposizione dall'Istituto.
F. Lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to-Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright.
G. Utilizzare servizi o risorse di rete, storage o calcolo, collegare apparecchiature o servizi o software alla rete, qualora queste azioni danneggino, arrechino disturbo o anche solo perturbino le attività di altre persone, utenti o servizi
H. Lo scaricamento di software o di aggiornamenti di software dei dispositivi personali degli Utenti, fatto salvo il caso dei tablet concessi dall’istituto in comodato d’uso gratuito (a tal proposito si chiede in particolare di impostare sui dispositivi personali l’orario degli aggiornamenti automatici al di fuori dell’orario di permanenza dell'Istituto).
I. Svolgere sulla rete ogni altra attività vietata dalla legge dello Stato, dalla normativa internazionale, nonché dai regolamenti e dalle consuetudini ("Netiquette") di utilizzo delle reti e dei servizi di rete cui si fa accesso.

La registrazione di informazioni relative al traffico Internet, in ogni caso, avverrà in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni.
In caso di comportamenti difformi singoli o reiterati oppure anomalie verranno inoltrati preventivi avvisi collettivi di richiamo al rispetto delle regole. Qualora, nonostante i richiami generalizzati, perduri un indebito utilizzo della rete internet l'Istituto procederà all’invio di avvisi più circoscritti, e – solo se a seguito della gradualità dei controlli emergano fondati sospetti – verranno allora effettuati controlli nominativi o su singoli dispositivi e postazioni.
Per facilitare il rispetto delle predette regole, l'Istituto si riserva, per mezzo dell’amministratore di sistema, la facoltà di configurare specifici filtri che inibiscono l’accesso a siti o contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all’attività didattica (es. upload, restrizione nella navigazione, download di *file* o software).

L'eventuale conservazione di dati è effettuata per il tempo strettamente limitato al perseguimento di finalità organizzative e di sicurezza.

In ogni caso l'Istituto non può in alcun caso utilizzare sistemi da cui derivino forme di controllo indebito dell’attività dell’Utente. Per tali s’intendono, a titolo meramente esemplificativo e non esaustivo:
- la lettura e la registrazione sistematica dei messaggi di posta elettronica;
- la riproduzione e la memorizzazione sistematica delle pagine internet

visualizzate da ciascun Utente, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;
- la lettura e la registrazione dei caratteri inseriti tramite tastiera o dispositivi analoghi;
- l'analisi occulta di computer portatili o tablet affidati in uso.

ART. 12 GESTIONE E UTILIZZO DELL'ACCOUNT GW

1. Norme di utilizzo dell'account GW

Nell'ambito dell'attività didattica, possono venire usati i servizi della piattaforma GW come Google Classroom, Google Meet, Google Chat o altre piattaforme didattiche autorizzate (ad esempio la piattaforma Moodle dell'Istituto).
Le credenziali di accesso sono strettamente personali e non possono, per nessun motivo, essere comunicate ad altre persone, né cedute a terzi, poiché ogni attività non regolare sarà imputata al titolare dell'account.
L'Utente è responsabile delle attività del suo account e accetta di essere riconosciuto quale autore di qualunque tipo di interazione (messaggi in chat, consegne in classe virtuale, messaggi di posta elettronica,...) dal suo account.
L'Utente si impegna a non utilizzare i servizi per effettuare azioni e/o comunicazioni che arrechino danni a terzi o che violino le leggi ed i regolamenti d'Istituto vigenti, a non trasmettere o condividere informazioni che possano presentare forme o contenuti di carattere pornografico, osceno, blasfemo, diffamatorio o contrario all'ordine pubblico o alle leggi vigenti in materia civile, penale ed amministrativa.
L'Utente si impegna ad utilizzare i servizi offerti dall'Istituto solo per finalità connesse alla propria attività didattica o comunque correlate con il processo educativo. In particolare, non è concesso l'utilizzo dell'account istituzionale per la partecipazione a dibattiti, forum, mail-list non attinenti la didattica o per la registrazione ad app e servizi web non autorizzati.

2. Norme di utilizzo della piattaforma GW

Riguardo all'utilizzo delle applicazioni del GW, l'Utente si impegna a:
- non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma GW con il proprio account;
- non comunicare il codice di accesso alla Google Classroom a coloro che non ne fanno parte;
- accettare e rispettare le regole del comportamento all'interno della classe virtuale e le normative nazionali vigenti in materia di utilizzo di materiali in ambienti digitali;
- non pubblicare immagini, per attività didattiche o extra-didattiche all'interno della classe virtuale senza previa autorizzazione dell'insegnante titolare della classe stessa. L'Utente si assume la piena responsabilità di tutti i dati inoltrati, creati e gestiti attraverso il proprio account GW istituzionale;
- non diffondere eventuali informazioni riservate di cui venisse a conoscenza, relative all'attività delle altre persone che utilizzano il servizio.

3. La posta elettronica istituzionale

Gli Utenti del servizio di posta elettronica collegata al proprio account GW istituzionale si impegnano ad utilizzare la propria casella di posta elettronica in modo responsabile, rispettando le leggi e secondo normali standard di cortesia, correttezza, buona fede e diligenza. Le **linee guida** per le comunicazioni interpersonali tramite l'email istituzionale (*Netiquette*) sono riportate nell'**Allegato B** del presente regolamento.

Si ricorda che, salvo l'utilizzo di appositi strumenti di cifratura, i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto, si richiede agli utenti di valutare con attenzione l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale".

4. Cessazione dell'indirizzo di posta elettronica istituzionale

La cessazione dell'indirizzo di posta istituzionale dell'Utente è subordinata alla cessazione dell'account GW, secondo le modalità indicate nell'Art. 8 del presente regolamento.

ART. 13 VIOLAZIONI

A fronte di violazioni del presente Regolamento da parte dell'Utente, l'insegnante titolare della classe virtuale, o il docente coordinatore, o l'Amministratore o il Dirigente scolastico comunicherà in modo orale e/o scritto quanto accaduto alla famiglia. L'accaduto sarà anche comunicato al Consiglio di Classe che ne potrà tener conto nel determinare il voto di condotta o per prendere altri provvedimenti in conformità con il Regolamento d'Istituto, il Patto di Corresponsabilità e il Regolamento Disciplinare adottati dall'Istituto.
Preso atto della violazione, e del parere espresso dall'insegnante titolare della classe virtuale e/o del Consiglio di Classe, il Dirigente Scolastico potrà sospendere l'account dell'utente e impedirne l'accesso immediato alla piattaforma per un periodo o revocarlo in modo definitivo senza alcun preavviso e senza alcun addebito a suo carico e fatta salva ogni altra azione di rivalsa nei confronti dei responsabili di dette violazioni.

L'Istituto dovrà, inoltre, informare le autorità competenti nel caso di reato, o presunto tale, compiuto tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici scolastici.

ART. 14 INFORMATIVA AGLI UTENTI

Il presente disciplinare interno, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici scolastici, nonché per l'uso di dispositivi personali nello svolgimento dell'attività didattica, e relativamente ai trattamenti di dati personali svolti dall'Istituto e finalizzati alla effettuazione di controlli leciti, così come definiti

nell’art. 5, vale quale informativa ex. art. 13 del Regolamento UE 2016/679 e successiva regolamentazione D. Lgs. 101/2018, così come disposta dal punto 3.3 delle Linee Guida del Garante Privacy del 1 marzo 2007.

ART. 15 COMUNICAZIONI

Il presente disciplinare interno è messo a disposizione degli utenti, per la consultazione, al momento dell’assegnazione di un account Utente. Nel sito web dell’Istituto è pubblicata la versione più aggiornata dello stesso allo scopo di facilitare la conoscibilità a tutti gli interessati. Ad ogni aggiornamento del presente documento, ne sarà data comunicazione tramite l’invio di apposito messaggio e-mail o tramite registro elettronico. Tutti gli utenti sono tenuti a conformarsi alla versione più aggiornata del presente disciplinare.

ART. 16 APPROVAZIONE DEL REGOLAMENTO

Il presente regolamento è stato approvato dal Consiglio di Istituto nella seduta del 22 novembre 2024

Allegato A

Criteri per la definizione delle password di account studente

L'Utente, nel definire il valore della password, deve rispettare le seguenti regole:

- utilizzare almeno **8 caratteri alfanumerici**, inclusi i caratteri speciali (#, %, etc.), di cui almeno uno numerico;
- la password deve contenere almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo “@#§£$%...”;
- non includere parti del nome, cognome, data di nascita e/o comunque elementi a lui agevolmente riconducibili;
- evitare l'utilizzo di password comuni e/o prevedibili;
- non riutilizzare la stessa password adoperata in altre app o servizi web

Attivazione verifica in due passaggi

L'Utente, per aggiungere un livello di sicurezza al proprio account Google Workspace, può attivare la verifica in due passaggi, chiamata anche autenticazione a due fattori. Ulteriori informazioni e le istruzioni per l’attivazione del servizio sono disponibili alla pagina:
https://support.google.com/accounts/answer/185839?hl=IT

Allegato B

Linee guida per le comunicazioni interpersonali (Netiquette)

- Non è consentito pubblicare, senza l'esplicito permesso dell'autore, il contenuto di messaggi di posta elettronica
- Rispettate la privacy del mittente/destinatario, cancellando dal testo della mail eventuali indirizzi di posta elettronica o riferimenti personali altrui nel caso in cui la mail dovesse essere inoltrata a un destinatario diverso da quelli originariamente inseriti.
- Utilizzate il campo CC (copia conoscenza) mettendo al massimo due destinatari che si conoscono tra loro o che dobbiamo presentare, altrimenti utilizzare il campo CCn. Se è necessario inviare informazioni a molti destinatari è consigliato creare una lista di distribuzione (gruppo di destinatari).
- Utilizzate il campo CCn (copia conoscenza nascosta) se è necessario inviare la stessa mail a destinatari diversi che non si conoscono tra loro.
- Scrivete sempre l'oggetto della mail, perché è cortese dare la possibilità al destinatario di sapere a colpo d'occhio la motivazione per cui gli avete scritto.
- Utilizzare la funzione programma l'invio in modo che le email vengano inviate durante l'orario scolastico o di lavoro del destinatario, evitando, salvo casi di urgenza o diversi accordi tra mittente e destinatari, comunicazioni durante il fine settimana o in orari serali.
- Non inviare tramite posta elettronica messaggi pubblicitari o comunicazioni che non siano stati sollecitati in modo esplicito.
- La posta elettronica è facilmente intercettabile quindi non scrivere mai dati confidenziali come carte di credito, password, etc. In caso di necessità utilizzare dei programmi di crittografazione.
- Ci sono questioni particolarmente complesse per cui la posta elettronica andrebbe evitata, preferendo comunicazioni più dirette, come una telefonata o un incontro di persona, laddove possibile.
- È cortesia rispondere a una mail entro 24-48 ore dalla sua ricezione.
- Non inviare o inoltrare mai lettere a catena via posta elettronica.
- Verificare gli indirizzi di cc: quando si risponde. È inutile continuare ad includere questi ultimi se il messaggio è diventato una conversazione tra due persone soltanto.
- Usare maiuscole e minuscole. SOLTANTO CON LE MAIUSCOLE È COME SE SI STESSE URLANDO.
- Nel caso ci si trovi in disaccordo con una persona, meglio proseguire la discussione attraverso e-mail personali piuttosto che nella lista o nel gruppo.

Linee guida per i gruppi

L'invio di email ai gruppi globali (tutti.docenti, tutti.studenti, tutti.ata) è riservato a comunicazioni **strettamente istituzionali** e deve essere autorizzato dal Dirigente scolastico. A queste email non è in genere opportuno rispondere; in caso di necessità si può contattare il mittente del messaggio, ma senza coinvolgere nella comunicazione l'intero gruppo

Allegato C

White list dei servizi e app di terze parti autorizzati

App o servizio	Accesso ai dati GW dell'account	
	Info profilo	Accesso ad altri dati
Moodle Liceo Copernico	SI	NO
Servizi Web	SI	NO
Copernicorsi	SI	NO
Overleaf	SI	NO
Adobe Scan	SI	NO
AutoDesk (CAD, Tinkercad, Fusion 360, ...)	SI	NO

Nota: In caso di cessazione dell'account (termine degli studi o trasferimento presso altro istituto,...) l'accesso ai siti web delle case editrici potrebbe essere sospeso o cancellato, con la conseguente perdita dei diritti d'accesso ai libri e alle risorse digitali (anche se regolarmente acquistati).

Lista servizi Google aggiuntivi attivati

SERVIZI AGGIUNTIVI
Applied Digital Skills
Chrome Web Store
Google Arts and Culture
Google Gruppi
Google Foto
Google Play
Google Traduttore
Motore di ricerca programmabile

Youtube
Podcast
Google Colab
Google Earth
Blogger
Profili Scholar

Aggiornamento del 20 giugno 2024