CONVITTO NAZIONALE di STATO "T. CAMPANELLA"

Scuole statali annesse: Primaria - Secondaria I grado – Liceo Classico - Classico Europeo

Via Aschenez, 180 - 89125 Reggio Cal. – C.M.: RCVC010005 – C.F.: 92093030804
Tel. 0965 499421 - Fax 0965 332253 – Sito web: www.convittocampanella.edu.it E-mail: rcvc010005@istruzione.it PEC: rcvc010005@pec.istruzione.it

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI, DEI DISPOSITIVI PERSONALI E DELLA CONNESSIONE INTERNET



Approvato con delibera del Collegio dei docenti del 12/11/2025 e adottato dal Consiglio di Istituto gestione commissariale il 24/11/2025 e confermato con delibera del Collegio dei Docenti del 14/09/2026

Il presente documento costituisce la riformulazione normativa e tecnica del Regolamento per l'utilizzo degli strumenti informatici, dei dispositivi personali e della connessione internet del Convitto Nazionale di Stato "T. Campanella". Il Regolamento mira a stabilire un quadro di riferimento chiaro per l'uso consapevole, sicuro e responsabile delle tecnologie digitali, in piena coerenza con la normativa italiana ed europea in materia di privacy, sicurezza sul lavoro e contrasto al cyberbullismo.

SEZIONE I: PRINCIPI FONDAMENTALI E QUADRO NORMATIVO

Art. 1 – Premessa, Fonti normative, Finalità.

1.1 Premessa

Il presente Regolamento definisce le modalità di utilizzo delle attrezzature informatiche, dei dispositivi personali e della connessione Internet messi a disposizione dal Convitto. L'obiettivo è promuovere un uso consapevole, sicuro e responsabile delle tecnologie digitali, in coerenza con il Piano Triennale dell'Offerta Formativa (PTOF), il Regolamento di Istituto e la normativa vigente in materia di privacy e sicurezza dei dati personali.

L'Istituto favorisce iniziative di sensibilizzazione e formazione rivolte a studenti, docenti e personale, anche in collaborazione con le famiglie e con enti esterni, al fine di sviluppare competenze digitali e comportamenti corretti nell'ambiente online.

Particolare attenzione è rivolta alla prevenzione del cyberbullismo, al rispetto reciproco nelle interazioni digitali e all'educazione alla sicurezza in rete.

Le disposizioni del presente Regolamento si applicano a tutti i membri della comunità scolastica (studenti, docenti, personale ATA e collaboratori esterni) e riguardano:

- le attrezzature informatiche di proprietà dell'Istituto (computer, tablet, LIM, stampanti, account istituzionali, piattaforme digitali, ecc.);
- i dispositivi personali utilizzati per finalità didattiche o comunque connesse all'attività scolastica;
- l'accesso e l'utilizzo della rete Internet e della connessione Wi-Fi dell'Istituto.

1.2 Fonti normative

- Costituzione della Repubblica Italiana, artt. 2, 3, 34.
- D.Lgs. 297/1994, Testo Unico della Scuola.
- D.P.R. 275/1999 (Regolamento Autonomia).
- D.Lgs. 81/2008 (tutela della salute e sicurezza nei luoghi di lavoro).
- Regolamento UE 2016/679 (GDPR).
- Legge 71/2017 e Legge 70/2024 (prevenzione e contrasto del cyberbullismo).
- Regolamento d'Istituto, Patto di corresponsabilità educativa, DVR.

1.3 Finalità

- Garantire un uso sicuro, controllato e lecito delle tecnologie.
- Tutelare i dati personali e prevenire abusi.
- Favorire un impiego didattico e amministrativo conforme agli obiettivi dell'Istituto.
- Attribuire responsabilità chiare a ogni utente.

SEZIONE II: GESTIONE DELLE RISORSE, ACCESSO, CUSTODIA E RESPONSABILITÀ

Art. 2 - Protocolli di Accesso e Tracciabilità

2.1. Requisiti di Accesso Obbligatori

L'accesso agli strumenti e alla rete scolastica è tassativamente consentito solo mediante l'utilizzo di account istituzionali. È severamente vietato l'uso di account personali o anonimi per l'esecuzione di attività didattiche o di servizio. Questo protocollo garantisce che ogni azione compiuta all'interno della rete scolastica sia riconducibile al soggetto che l'ha intrapresa.

2.2. Controllo e Monitoraggio Istituzionale

L'accesso alla rete e l'uso degli strumenti sono tracciati e monitorati attraverso appositi registri informatici. L'uso è autorizzato esclusivamente in funzione delle finalità didattiche o di servizio definite dall'Istituto. L'obbligo di tracciabilità, affiancato alla conservazione dei registri, eleva la registrazione d'uso da una semplice misura amministrativa a uno strumento legale cruciale. In caso di indagine o controversia (disciplinare, civile o penale), la tracciabilità forzata e la documentazione del login di accesso fungono da prova inconfutabile (relativa a tempo, luogo e identità dell'utente), consentendo una precisa e inoppugnabile attribuzione di responsabilità.

Art. 3 - Obblighi Documentali: Registri e Archiviazione

3.1. Tipologie di Registri Mandatori

L'Istituto impone la compilazione e la gestione di registri obbligatori volti a documentare l'utilizzo e la movimentazione delle risorse. Questi includono: il Registro di utilizzo dei laboratori informatici (che documenta prenotazioni e presenze), il Registro di concessione dei dispositivi (PC, tablet, LIM, ecc.), che richiede la firma di presa in carico e riconsegna, e il Registro degli accessi amministrativi alla rete e alle piattaforme digitali.

3.2. Modalità e Tempi di Conservazione

I registri devono essere conservati per un periodo non inferiore a 12 mesi dai responsabili designati tramite specifico provvedimento del Dirigente Scolastico. In particolare, l'attività laboratoriale deve essere meticolosamente registrata nel registro di prenotazione e presenze, con l'indicazione del docente responsabile, della classe e degli orari precisi di entrata e uscita dal laboratorio.

Art. 4 - Custodia dei Dispositivi Affidati e Regime di Responsabilità

4.1. Dovere di Diligenza e Responsabilità Primaria

Ogni utente cui viene affidato un dispositivo è tenuto a custodirlo con diligenza. La persona che firma il registro di presa in carico è riconosciuta come responsabile in prima persona della conservazione del bene fino alla sua riconsegna formale. Per quanto no espressamente disciplinato si fa rinvio alle disposizioni del Regolamento per il Comodato d'uso di Tablet e di Pc in vigore nel nostro istituto.

4.2. Responsabilità del Personale (Docenti e ATA)

In caso di smarrimento, furto, danneggiamento o uso improprio di un dispositivo affidato, l'utente affidatario (sia esso docente o personale ATA) risponde in termini sia civilistici che disciplinari.

4.3. Responsabilità degli Studenti e dei Genitori

Gli studenti, unitamente alle loro famiglie, sono ritenuti responsabili per eventuali furti, manomissioni, smarrimenti o usi impropri dei dispositivi scolastici, in conformità con la normativa vigente e il Regolamento d'Istituto. L'Istituto mitiga il rischio patrimoniale trasferendo esplicitamente la responsabilità della custodia all'atto dell'affidamento. Il **Registro di concessione dei dispositivi** (Art. 3.1) è pertanto un documento essenziale per formalizzare il momento esatto in cui avviene il trasferimento di custodia, permettendo all'Istituto di gestire con precisione le richieste risarcitorie in caso di danno.

SEZIONE III: MISURE DI SICUREZZA, DATI E CONDOTTE PROIBITE

Art. 5 - Usi Proibiti, Diritti di Proprietà Intellettuale e Rispetto Etico

5.1. Divieto di alterazione tecnica e contenuti illeciti

È fatto assoluto divieto di installare software non autorizzato o di modificare le configurazioni dei dispositivi di proprietà dell'Istituto. È altresì proibito accedere a siti web che veicolino contenuti vietati, violenti, discriminatori, pornografici o comunque non pertinenti all'attività didattica o di servizio.

5.2. Proprietà Intellettuale e Uso Personale

È vietato scaricare, duplicare o utilizzare materiale privo di licenza o protetto da copyright. L'utilizzo di chat, social network o posta elettronica per fini strettamente personali è proibito su tutti i dispositivi e le reti dell'Istituto.

Art. 6 - Divieti di Registrazione, Diffusione Multimediale e Protezione della Dignità

6.1. Divieto assoluto di registrazione e diffusione

Per la tutela della privacy e della dignità personale, è assolutamente vietato registrare, fotografare o diffondere immagini, video e audio riferibili a studenti, docenti o personale scolastico senza un esplicito e preventivo consenso. L'uso della fotocamera o del microfono integrati nei dispositivi, siano essi scolastici o personali, non è consentito senza specifica autorizzazione del docente responsabile.

Qualsiasi raccolta, registrazione o diffusione non autorizzata di dati personali (quali immagine o voce) configura un "trattamento illecito di dati personali". Tale violazione, oltre alle immediate sanzioni disciplinari, può avere ripercussioni penali gravi, come previsto dagli Artt. 167 e seguenti del Codice Privacy.

6.2. Condotte Digitali che costituiscono violazione della dignità (Cyberbullismo)

È vietato l'utilizzo degli strumenti informatici, piattaforme digitali o social network per: diffondere contenuti offensivi, discriminatori o denigratori verso compagni, docenti, personale scolastico o terzi; creare o condividere materiale multimediale non autorizzato che violi la privacy o la dignità delle persone; o attuare atti di esclusione, intimidazione o minaccia a mezzo digitale. Si richiama il Regolamento Bullismo e Cyberbullismo in vigore nel nostro istituto.

Art. 7 - Sicurezza e Trattamento dei Dati Personali (GDPR)

7.1. Obblighi di sicurezza tecnica

In ottemperanza al GDPR (Art. 32) e al D.Lgs. 81/2008, tutti i dispositivi utilizzati a scuola, inclusi i BYOD, devono essere protetti da password robuste e da sistemi antivirus regolarmente aggiornati. La mancata adozione di tali misure di sicurezza di base è considerata una violazione delle norme interne che espone l'utente a responsabilità disciplinare e civile.

7.2. Principio di minimizzazione dei dati

Al fine di rispettare il principio di minimizzazione dei dati sancito dal GDPR, è vietato archiviare o trattare dati sensibili o personali su dispositivi personali o non protetti. La violazione di questa norma può integrare un illecito trattamento di dati personali, con conseguenze che possono estendersi anche alla sfera penale.

7.3. Ruolo di filtro e monitoraggio dell'Istituto

L'Istituto è tenuto ad adottare sistemi di filtro e monitoraggio per impedire accessi indebiti e garantire le misure di sicurezza tecniche previste dall'Art. 32 del GDPR. È fondamentale sottolineare che tali controlli, pur essendo necessari, non esimono studenti e genitori dalla responsabilità individuale per comportamenti scorretti o illeciti.

7.4. Obbligo di segnalazione delle violazioni (Data Breach)

Ogni violazione del regolamento o sospetto incidente di sicurezza (uso improprio, attacco informatico, accesso non autorizzato o episodio di cyberbullismo) deve essere segnalata **senza ritardo** al Dirigente Scolastico e al Data Protection Officer (DPO). Tale obbligo di notifica delle violazioni è previsto specificamente dagli Artt. 33 e 34 del GDPR.

SEZIONE IV: DISPOSIZIONI SPECIFICHE PER AMBIENTI E DISPOSITIVI

Art. 8 - Uso dei Laboratori Informatici

8.1. Utilizzo del Laboratorio fisso o mobile

Per laboratorio fisso si intende qualsiasi spazio scolastico dotato di attrezzature specifiche destinate ad attività pratiche o sperimentali. Per laboratorio mobile si intende un'attrezzatura didattica flessibile e portatile che porta risorse scientifiche, digitali o artistiche direttamente nelle aule, superando le limitazioni dei laboratori fissi. Il Dirigente Scolastico provvede annualmente alla nomina del personale responsabile dei laboratori, eventualmente supportati dagli assistenti tecnici. I responsabili hanno il compito di sovrintendere alla gestione, alla sicurezza e al rispetto di tutte le norme d'uso.

8.2. Applicazione delle Norme Generali

La violazione delle regole d'uso può comportare l'esclusione temporanea o definitiva dall'accesso al laboratorio, oltre alle sanzioni disciplinari e civili previste.

Art. 9 - Uso della Rete Internet e della Posta Elettronica Istituzionale

9.1. Restrizione Funzionale

È imposto l'assoluto divieto di utilizzare la connessione Internet e la posta elettronica istituzionale per fini personali. L'uso è consentito esclusivamente per l'espletamento delle attività didattiche e istituzionali.

9.2. Divieti Specifici

È vietato l'invio di messaggi di spam, di comunicazioni offensive o discriminatorie e qualsiasi forma di uso improprio dei dati personali attraverso la rete scolastica.

SEZIONE V: VIGILANZA, RESPONSABILITÀ DEL PERSONALE E SANZIONI

Art. 10 - Utilizzo dei Telefoni Cellulari da Parte di Docenti e Personale ATA

10.1. Obblighi e Divieti per il Personale Docente, alunni e il Personale ATA.

L'uso di telefoni cellulari e dispositivi personali da parte di docenti e personale ATA è consentito esclusivamente per esigenze di servizio, motivi di sicurezza o comunicazioni istituzionali autorizzate. Durante le ore di lezione, è fatto divieto ai docenti di utilizzare il cellulare per motivi personali, al fine imprescindibile di garantire la continuità didattica e la vigilanza sugli alunni. L'uso personale è ammesso solo in situazioni urgenti e motivate (es. registro elettronico, emergenze sanitarie, comunicazioni con il Dirigente). Il personale ATA può utilizzare il cellulare esclusivamente per esigenze di servizio (comunicazioni interne, emergenze, registrazioni di dati organizzativi). Per gli alunni si rimanda all'art. 16 del Regolamento di Istituto.

L'uso del cellulare per fini personali durante l'orario di servizio costituisce un elemento di **distrazione dall'obbligo di sorveglianza** e comporta l'immediata responsabilità disciplinare. Per quanto non espressamente disciplinato si richiama il Regolamento di Istituto.

10.2. Divieto Trasversale di Registrazioni

Come ribadito dall'Art. 6.1, è assolutamente vietato l'uso dei cellulari per fotografare, registrare audio/video o diffondere immagini e dati riferibili a studenti, docenti o personale senza autorizzazione del Dirigente Scolastico, in conformità al GDPR e al D.Lgs. 196/2003.

Art. 11 - Obbligo di Vigilanza Attiva e Responsabilità del Docente

11.1. Requisito della Vigilanza Attiva

L'uso di dispositivi digitali e l'accesso alla rete scolastica da parte degli studenti sono consentiti esclusivamente in presenza e sotto la **vigilanza attiva** di un docente. Il docente in servizio è responsabile della sorveglianza degli alunni e deve vigilare attivamente che i dispositivi siano

impiegati solo per fini educativi, impedendo deviazioni immediate verso attività estranee o rischiose (come giochi, social network o contenuti illeciti).

L'istituto stabilisce un elevato standard di cura digitale, richiedendo che la vigilanza non sia solo fisica ma attiva sul contenuto e sulla condotta digitale. L'omissione di questa sorveglianza attiva, specialmente in un ambiente digitale dove il danno può propagarsi istantaneamente, viene qualificata come colpa grave. Questa definizione rafforza la posizione dell'Istituto in caso di richieste risarcitorie per danni a persone o cose causati dalla mancata intercettazione di un comportamento illecito. Il personale ATA è tenuto a collaborare segnalando tempestivamente usi impropri o anomalie. È proibito lasciare dispositivi accesi o incustoditi negli spazi comuni.

11.2. Conseguenze in Caso di Mancata Vigilanza

In caso di mancata vigilanza, il docente può essere chiamato a rispondere disciplinarmente secondo quanto previsto dal CCNL e civilmente nei casi di danno a persone o cose derivanti da colpa grave o dolo. Gli studenti che utilizzano i dispositivi senza autorizzazione o in assenza di un docente incorrono in sanzioni disciplinari previste dal Regolamento di disciplina e nell'obbligo di risarcimento dei danni arrecati.

Art. 12 - Sanzioni e Procedimenti Disciplinari

12.1. Sanzioni per gli Studenti

L'Istituto, inoltre, recepisce la Legge 71/2017 e la Legge 70/2024, che sanciscono la tutela dei minori e la responsabilità della scuola nella prevenzione e contrasto del cyberbullismo.

Le violazioni del Regolamento comportano le seguenti conseguenze per gli studenti: ammonizione formale con contestuale revoca dell'autorizzazione all'uso delle tecnologie e dei laboratori; sanzioni disciplinari previste dal Regolamento d'Istituto (che possono giungere fino alla sospensione dalle lezioni); obbligo di risarcimento per danni materiali o morali; e, nei casi più gravi, segnalazione diretta alla Polizia Postale o all'Autorità Giudiziaria competente. Per quanto non espressamente disciplinato si richiama il Regolamento di Istituto e il Regolamento Bullismo e Cyberbullismo.

12.2. Sanzioni per Docenti e Personale ATA

L'uso improprio di dispositivi o la mancata segnalazione di episodi accertati contrari al Regolamento da parte di docenti e personale ATA comporta l'attivazione dei procedimenti disciplinari previsti dal CCNL Scuola e dal Codice di comportamento dei dipendenti pubblici (D.P.R. 62/2013). Nei casi più gravi, come la diffusione non autorizzata di immagini, violazioni gravi della privacy, cyberbullismo attivo o mancata vigilanza con gravi conseguenze sugli alunni, il Dirigente scolastico procederà con la segnalazione alle autorità competenti. Per quanto non espressamente disciplinato si richiama il Regolamento di Istituto.

12.3. Disposizioni Finali

Il presente Regolamento è valido a partire dall'anno scolastico 2025/2026. Esso è parte integrante del PTOF, del Regolamento d'Istituto e del Patto di corresponsabilità educativa. Per quanto non espressamente disciplinato, si fa rinvio alle disposizioni generali del Regolamento d'Istituto.

Il Dirigente Scolastico
dr.ssa Francesca Arena
documento informatico firmato digitalmente
ai sensi del D.Lgs 82/2005 s.m.i. e norme collegate
il quale sostituisce il documento cartaceo e la firma autografa