



REPUBBLICA ITALIANA – REGIONE SICILIANA

Istituto di Istruzione Superiore “Fratelli Testa”

Viale Itria 2/A - 94014 Nicosia (EN) - Tel.: 0935647258 - Fax 0935630119

C.F. 91052080867 - C.M. ENIS01900T

e-mail: [enis01900t@istruzione.it](mailto:enis01900t@istruzione.it)

<http://www.liceotesta.it> ::

p.e.c.: [enis01900t@pec.istruzione.it](mailto:enis01900t@pec.istruzione.it) ::

Nicosia, 22/04/2026

Circolare n. 241

A.S. 2025-2026

Al Personale Docente

e p.c.

Al DSGA

Al personale ATA

All'Amministratore di Sistema

## Oggetto: Utilizzo dei sistemi informatici, delle risorse digitali ed audiovisive dell'Istituto

Con la presente, si forniscono le indicazioni operative e linee di condotta riguardanti l'uso dei sistemi informatici, delle apparecchiature digitali ed audiovisive e delle risorse online messe a disposizione dall'Istituto, nell'ottica di un utilizzo sicuro, responsabile e coerente con gli obiettivi protezione dei dati, di didattica digitale ed amministrazione.

Inoltre sono stati rinnovati tutti gli adempimenti previsti dalla legge in materia di privacy in ottemperanza al GDPR (lettere di incarico al trattamento dei dati a docenti/ATA/personale esterno/fornitori, informative, etc), stante l'avvenuto cambio del Responsabile del Trattamento dei dati nella persona del Dirigente scolastico pro-tempore.

A tal fine si fa rilevare che l'Agenzia per la Cybersicurezza Nazionale (ACN) istituita dal Decreto Legge n.82 del 14 giugno 2021, con riferimento al 1° semestre 2025, ha censito **1.549 eventi di cybersicurezza**, segnando un **aumento del 53%** degli incidenti informatici rispetto allo stesso periodo del 2024. Molti di questi eventi riguardano i sistemi informativi dello Stato, fra i quali quelli del Ministero dell'Istruzione e del Merito che ha istituito una apposita struttura denominata CSIRT MIM (Computer Security Incident Response Team del Ministero dell'Istruzione e del Merito) che coordina la sicurezza informatica del Ministero, degli USR e delle Scuole dislocate in tutto il territorio nazionale.

### 1. Ambito di applicazione

Le disposizioni contenute nella presente circolare si applicano a tutto il personale docente e ATA che utilizza le risorse informatiche dell'Istituto, incluse: rete LAN / WiFi, postazioni pc, account di posta elettronica istituzionale, piattaforme cloud o di collaborazione digitale, strumenti di comunicazione online.

Specifiche ed ulteriori indicazioni saranno fornite, con successiva comunicazione, al personale ATA, ai Collaboratori vicari del Dirigente Scolastico ed a determinate funzioni strumentali.

## 2. Obiettivi della circolare

- Garantire la disponibilità, integrità e riservatezza delle informazioni e, soprattutto, la sicurezza informatica della rete informatica di Istituto.
- Promuovere l'uso consapevole e professionale delle tecnologie digitali nella didattica e nel lavoro amministrativo.
- Tutelare la privacy degli alunni, del personale e dei dati gestiti, in conformità al quadro normativo vigente (Regolamento UE 2016/679 – GDPR, D.Lgs. 82/2005 “Codice dell'Amministrazione Digitale”).
- Favorire un clima di uso responsabile delle tecnologie, in linea con il progetto di digitalizzazione dell'istituto.

## 3. Regole generali di utilizzo della rete di istituto

- a) Gli account, le password e gli accessi assegnati dall'Istituto sono personali e non devono essere condivisi per nessun motivo, anche laddove le credenziali di accesso siano condivise (PC delle classi, aule docenti, aree comuni)
- b) Le risorse digitali (hardware, software, rete, piattaforme) devono essere utilizzate esclusivamente per fini didattici ed amministrativi e mai per uso personale.
- c) È vietato utilizzare i sistemi per scopi non autorizzati, installare software non approvati o aggirare le misure di sicurezza all'uopo predisposte. Ogni docente deve segnalare tempestivamente, sempre e comunque in forma scritta, eventuali anomalie o accessi non autorizzati.
- e) I dati personali devono essere trattati nel rispetto della privacy e della sicurezza.
- f) È obbligatorio utilizzare solo piattaforme web approvate dall'Istituto (Google Workspace, Argo, ..)
- g) L'utilizzo della rete WiFi deve rispettare le policy interne e la netiquette digitale e su richiesta viene concessa in uso anche al personale in servizio presso l'Istituto, secondo le indicazioni ministeriali sul BYOD (Bring Your Own Devices) che disciplina l'utilizzo dei propri dispositivi personali (notebook, tablet, smatphone) connessi alla rete informatica di Istituto.
- h) E' severamente vietato accedere a sistemi informatici per i quali non si possiede autorizzazione esplicitata e formalizzata a mezzo lettera di nomina al trattamento dei dati.
- i) Ogni docente dispone di proprio spazio di archiviazione su cloud (Google Drive) sul dominio @liceotesta.it che è accessibile da qualunque postazione. Pertanto è vietato l'utilizzo di pen drive in quanto potenziale veicolo di diffusione di virus informatici all'interno della rete di Istituto

#### 4. Corretto utilizzo delle LIM e delle postazioni informatiche nelle classi

**Ai sensi dell'art. 29 del CCNL Scuola** il docente è tenuto ad adempiere ai compiti connessi con la funzione docente, tra cui “la cura e il corretto utilizzo dei mezzi didattici e degli strumenti affidati”

Pertanto durante la lezione in cui il docente che utilizza la LIM e/o il personal computer in dotazione alla classe:

- È responsabile della gestione della LIM, del Personal computer e degli accessori (pennarelli, cavi, ecc.);
- Il docente della prima ora deve accendere il sistema LIM/Personal Computer per verificarne il corretto funzionamento, per consentire l'aggiornamento automatico dei sistemi operativi (antivirus, patch di sicurezza, etc.) ed, eventualmente, segnalare eventuali guasti e/o anomalie al collaboratore scolastico di piano per un pronto ed efficace intervento da parte dei tecnici.
- Il docente dell'ultima ora deve verificare che il sistema LIM/Personal Computer venga spento correttamente al termine delle lezioni per evitare sprechi energetici, proteggere le lampade del pannello LCD e, in ultimo, per evitare danneggiamenti dovuti a spegnimenti impropri.
- Nel caso in cui si consenta agli alunni di utilizzare direttamente il sistema LIM/Personal Computer il docente deve vigilare sul corretto utilizzo da parte degli stessi.
- Il docente deve avere cura di non memorizzare credenziali personali di alcun tipo, in primis nomi utenti e password del portale Argo e della casella di posta elettronica istituzionale @liceotesta.it e @scuola.istruzione.it, anche al fine di prevenire il furto di identità digitale
- Il docente che si allontana dalla postazione lasciandola incustodita (ad es. per il cambio dell'ora, per la pausa di ricreazione, etc. ) deve disconnettere il profilo utente “Docente” riportandolo alla schermata di blocco con inserimento della password iniziale

Si fa rilevare che l'amministratore di sistema (vedi punto 10.), per motivi di sicurezza informatica sopravvenuta o programmata (incidenti informatici, virus, manutenzione ordinaria e/o straordinaria su hardware e software) costituenti prerogative di legge, ha facoltà senza preavviso di configurare, reinstallare software di sistema o applicativo, di eliminare dati di navigazione (cookie, cronologia, file temporanei), di eliminare il profilo denominato “Docente” con tutti i dati annessi e connessi (cartelle Desktop/Documenti/Download).

Ne discende che il docente non deve conservare dati in locale sul PC ma deve utilizzare il servizio di archiviazione su cloud (Google Drive), in quanto esso garantisce sicurezza sulla presenza di virus informatici e costante back-up dei dati nonché una disponibilità immediata degli stessi su qualunque postazione, organizzandone la struttura di archiviazione sulla base delle proprie esigenze personali.

E' altresì vietato a docenti e/o alunni di alterare la configurazione delle impostazioni hardware e software del sistema LIM/Personal Computer (sfondi del desktop, schermata di blocco, cambio password, disposizione delle icone)

## 5. Postazioni internet e di stampa dedicate ai docenti

Nelle aule docenti di tutti i plessi scolastici e nelle aree comuni (plessi Classico, Scientifico, Tecnico), sono attivate numerose postazioni di stampa dedicate, in via esclusiva, ai docenti in servizio presso ciascuna sede. In particolare, attualmente, sono attive le seguenti postazioni informatiche, che si ritengono più che adeguate alle esigenze d'uso in quanto a consistenza numerica e tecnologica:

### A) Plesso Liceo Classico:

AULA DOCENTI:

n. 4 postazioni internet di cui n. 3 dotate di stampante

AUDITORIUM:

n. 1 postazione internet

### B) Plesso Liceo Scientifico:

AULA DOCENTI:

n. 2 postazioni internet dotate di stampante (locale e di rete)

### C) Plesso Istituto Tecnico:

AULA DOCENTI:

n. 3 postazioni internet di cui n. 2 dotate di stampante

UFFICIO EX PRESIDENZA:

n. 2 postazione internet n. 1 dotata di stampante

Pertanto i docenti possono procedere in autonomia alle stampe strettamente necessarie alle attività didattiche, avendo cura di selezionare, ove possibile, la funzione di risparmio dell'inchiostro; in caso di inceppamento della macchina, altri malfunzionamenti o problemi tecnici, i Docenti avranno cura di rivolgersi al collaboratore scolastico di piano che provvederà ad informare tempestivamente l'Assistente tecnico referente di plesso; in mancanza di questi, i docenti adotteranno ogni possibile accorgimento e cautela al fine di risolvere i problemi contingenti senza mettere a rischio il macchinario.

In ogni caso, è bene ribadirlo,

## 6. Postazioni informatiche delle portinerie e della segreteria

Per inderogabili motivi di sicurezza informatica, stante la loro interconnessione diretta al sistema informativo di Segreteria, in nessun caso e per nessun motivo i docenti possono utilizzare i le

postazioni informatiche in dotazione ai collaboratori scolastici ed attivate nelle portinerie (Plesso liceo Classico piano terra e primo, Plesso liceo Scientifico piano terra, plesso istituto Tecnico piano terra), come pure è vietato l'utilizzo di qualsivoglia altra postazione in dotazione agli uffici di segreteria. E' fatta salva la deroga individuale formalizzata e motivata per iscritto dal Dirigente Scolastico per casi d'uso specifici (ad es. collaboratori del dirigente scolastico et similia) in ragione delle attribuzioni proprie della funzione rivestita all'interno dell'organigramma scolastico.

## **7. Centri elaborazioni dati**

E' severamente interdetto l'accesso ai locali sede dei Centri Elaborazione Dati dei singoli plessi (Classico e Tecnico) le cui porte di accesso sono contrassegnate con opportuni segnali di divieto assoluto di ingresso.

L'accesso a detti locali è consentito esclusivamente al personale ATA o, eventuale, al personale tecnico esterno preventivamente autorizzato.

## **8. Laboratori informatici**

L'utilizzo dei laboratori informatici di istituto è disciplinato da apposito Regolamento approvato dal Consiglio di istituto in data 20.02.2020, allegato in coda alla presente circolare (ALLEGATO 1) e della quale costituisce parte integrante.

I docenti che intendono utilizzare i laboratori (attività didattiche, prove invalsi, certificazione ECDL, progetti formativi extra-didattici) o che comunque sono individuati per effettuare sorveglianza in seno alle prove

INVALSI sono tenuti a leggere preventivamente copia del predetto Regolamento rendendone edotti anche gli alunni.

Copia cartacea del Regolamento è presente in ciascun laboratorio.

## **9. Auditorium**

L'accesso e l'utilizzo dell'Auditorium, tanto in via estemporanea quanto in eventi e manifestazioni didattiche e/o culturali, è consentito previa autorizzazione del Dirigente Scolastico, sentito il DSGA che ne verifica la disponibilità sulla base del calendario degli impegni della struttura, e va quindi richiesto con congruo anticipo (almeno 48 ore prima), salvo i rari casi di necessità ed urgenza (assemblee straordinarie et similia).

Per nessun motivo è consentito accedere in Auditorium senza la presenza di un assistente tecnico, che ne predispona le apparecchiature necessarie all'attività richiesta e programmata.

## **10. Amministratore di sistema**

L'amministratore di sistema è responsabile della **configurazione, gestione e sicurezza dei sistemi informatici e delle reti informatica della scuola**. In particolare l'amministratore di sistema ha il compito di:

- a) Applicare le indicazioni operative del CSIRT MIM (Computer Security Incident Response Team" del Ministero dell'Istruzione e del Merito), ovvero l'unità istituita per gestire la sicurezza informatica nell'ambito del Ministero.
- b) installare e configurare sistemi operativi, server e reti;
- c) gestire utenti, permessi e risorse informatiche e tecnologiche;
- d) monitorare e ottimizzare le prestazioni dei sistemi;
- e) garantire la sicurezza dei dati e delle infrastrutture;
- f) effettuare backup e aggiornamenti;
- g) risolvere guasti e problemi tecnici.
- h) Tenere i rapporti con i fornitori di connettività, hardware e software
- i) Fornire indicazioni operative agli utenti (DS, DSGA, Docenti, della rete scolastica

Dall'a.s. 2019/20 questa Scuola ha individuato e confermato anche nel corrente anno scolastico quale Amministratore di sistema il dr. Giuseppe Rossino, già assistente tecnico di area informatica in servizio presso in nostro Istituto.

## 11. Didattica digitale e strumenti collaborativi

I docenti sono invitati a selezionare risorse coerenti con gli obiettivi formativi, promuovere un uso consapevole delle tecnologie e utilizzare esclusivamente strumenti autorizzati dall'Istituto per attività digitali e a distanza.

## 12. Formazione e aggiornamento

I docenti sono invitati a partecipare alle iniziative di formazione organizzate dall'Istituto in tema di sicurezza informatica, didattica digitale, privacy e strumenti di collaborazione online.

Questa Dirigenza intende avviare un ciclo di interventi formativi a beneficio di Docenti/Alunni/ATA inerenti le tematiche sopra menzionate finalizzate ad un utilizzo efficace, sicuro e produttivo delle moderne tecnologie informatiche e telematiche (Software applicativi, Reti, Cloud computing, Intelligenza Artificiale generativa)

### 13. Responsabilità e sanzioni

L'Istituto potrà adottare misure disciplinari in caso di uso improprio dei sistemi informatici. Ogni docente resta responsabile del corretto utilizzo delle risorse assegnate.

L'Istituto si riserva di adottare le misure necessarie in caso di uso improprio o illecito delle risorse informatiche che possa compromettere la sicurezza della rete, dei dati o la regolare attività didattica e amministrativa.

Si ricorda che l'accesso o l'utilizzo di un sistema informatico o telematico senza la necessaria autorizzazione costituisce reato ai sensi dell'art. 615-ter del Codice Penale ("Accesso abusivo a un sistema informatico o telematico"), punito con la reclusione da sei mesi a tre anni, pena che può aumentare in caso di aggravanti (es. pubblica amministrazione, violazione di sistemi protetti o alterazione dei dati). Analogamente, la diffusione di codici di accesso, la manipolazione di dati o l'intercettazione di comunicazioni informatiche possono configurare ulteriori reati previsti dal Codice Penale (artt. 617- quater, 617-sexies, 635-bis e seguenti).

Pertanto, ogni docente è personalmente responsabile del corretto utilizzo delle proprie credenziali e delle risorse assegnate sulla base della presente circolare, e deve astenersi da qualsiasi attività che possa compromettere la sicurezza o l'integrità dei sistemi informatici dell'Istituto.



**La Dirigente Scolastica**

Dott.<sup>ssa</sup> *Giuseppa Giambirtone*

(Firma autografa sostituita a mezzo stampa  
ai sensi dell'art. 3, comma 2 del D.Lgs. 39/93)