ISTITUTO DI ISTRUZIONE SUPERIORE PERITO-LEVI
Liceo Classico – Liceo Artistico - Liceo Musicale - Liceo Classico Europeo
Via E. Perito, 20 - Eboli (SA) Tel. 0828/366586 C.M. SAIS059003
Cod. Fiscale 91053310651- www.iisperitolevi.edu.it CODICE UNIVOCO UFFICIO:UF84TA
Sede Levi - Via Pescara, 10 - Eboli (SA) Tel. 0828/366793
sais059003@istruzione.it - sais059003@pec.istruzione.it
DISTRETTO SCOLASTICO N.57 - AMBITO SA-26

I.I.S. - "PERITO - LEVI" -Eboli (SA)
Prot. 0010755 del 28/08/2026
I (Uscita)

AL PERSONALE
AGLI INTERESSATI
AL DSGA
ALBO
ATTI

SEDE

OGGETTO: DISCIPLINARE PER L'UTILIZZO DEGLI STRUMENTI INFORMATICI, DI INTERNET E DELLA POSTA ELETTRONICA

e principali misure di sicurezza informatica
adottato ai sensi del Reg. (UE) 2016/679 (GDPR), del Codice in materia di protezione dei dati personali,
del codice di comportamento dei dipendenti pubblici e delle misure minime di sicurezza ICT per le PA

Sommario

1. Premessa e finalità

La diffusione delle tecnologie dell'informazione rappresenta una risorsa essenziale per l'attività dell'Istituzione scolastica, ma richiede di contemperare le esigenze organizzative e di sicurezza dell'Amministrazione con la tutela della riservatezza e della dignità del personale. Il presente Disciplinare definisce le regole per il corretto utilizzo degli strumenti informatici, di Internet e della posta elettronica messi a disposizione dall'Istituzione scolastica, nonché le principali misure di sicurezza, in coerenza con le indicazioni del Garante per la protezione dei dati personali in materia di trattamento dei dati del personale.

L'Istituzione scolastica è **Titolare del trattamento** dei dati personali trattati con tali strumenti; il Dirigente Scolastico ne è il legale rappresentante ed è affiancato dal Responsabile della protezione dei dati (DPO). Il Disciplinare è elaborato per: indicare i criteri di corretto utilizzo degli strumenti da parte del personale; definire i limiti e le finalità entro cui l'Amministrazione può effettuare controlli; fornire al personale istruzioni operative valide anche ai sensi dell'art. 32, par. 4, del GDPR.

Le regole del presente Disciplinare costituiscono **istruzioni impartite dal Titolare** e hanno valore di ordine di servizio: il loro mancato rispetto può dar luogo a responsabilità disciplinare ai sensi della vigente normativa contrattuale (CCNL del Comparto Istruzione e Ricerca), del D.Lgs. 165/2001, del D.P.R. 62/2013 e del codice di comportamento integrativo dell'Istituto. Il Disciplinare integra e completa l'informativa sul trattamento dei dati del personale resa ai sensi dell'art. 13 del GDPR.

2. Quadro normativo di riferimento

- Reg. (UE) 2016/679 (GDPR) e D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018 (Codice in materia di protezione dei dati personali);
- D.Lgs. 7 marzo 2005, n. 82 (CAD) e ss.mm.ii., in particolare l'art. 12, comma 3-bis, sull'uso di dispositivi elettronici personali;
- D.P.R. 28 dicembre 2000, n. 445 (TUDA);
- D.P.R. 16 aprile 2013, n. 62 (Codice di comportamento dei dipendenti pubblici), come modificato dal **D.P.R. 13 giugno 2023, n. 81**, che ha introdotto gli artt. 11-bis (utilizzo delle tecnologie informatiche) e 11-ter (utilizzo dei mezzi di informazione e dei social media), in attuazione dell'art. 4 del D.L. 36/2022 (conv. L. 79/2022);
- D.Lgs. 30 marzo 2001, n. 165 e CCNL del Comparto Istruzione e Ricerca, in materia di rapporto di lavoro e doveri del pubblico dipendente, nonché il codice di comportamento integrativo dell'Istituto;
- Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori), in particolare l'art. 4 in materia di strumenti di lavoro e controlli a distanza, e l'art. 8;
- Circolare AgID 18 aprile 2017, n. 2/2017 (Misure minime di sicurezza ICT per le pubbliche amministrazioni) e Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici;
- Legge 28 giugno 2024, n. 90 (rafforzamento della cybersicurezza nazionale e reati informatici) e D.Lgs. 4 settembre 2024, n. 138 (recepimento della Direttiva NIS2), quale cornice di riferimento per la sicurezza informatica e la gestione degli incidenti;
- Garante per la protezione dei dati personali, Provvedimento del 6 giugno 2024, n. 364 (Documento di indirizzo sui programmi di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati), e Provvedimento dell'1 marzo 2007, n. 13 (Linee guida posta elettronica e internet);

- Legge 23 dicembre 1993, n. 547 e artt. 615-ter ss. del Codice penale (reati informatici); Legge 22 aprile 1941, n. 633 (diritto d'autore, software e banche dati).

3. Ambito di applicazione e destinatari

Il Disciplinare si applica a tutto il personale dell'Istituzione scolastica — Dirigente Scolastico, D.S.G.A., personale docente e personale ATA — nonché ai collaboratori e a ogni altro soggetto autorizzato che, a qualunque titolo, utilizzi gli strumenti informatici, la rete e i servizi dell'Istituto. Le risorse di calcolo, memorizzazione e trasmissione (postazioni di lavoro, dispositivi mobili, rete, account, posta elettronica, applicativi) sono di proprietà dell'Istituzione scolastica e sono affidate al personale in uso non esclusivo e temporaneo, per il solo svolgimento delle attività istituzionali e nei limiti delle mansioni assegnate.

4. Principi generali di utilizzo

Il personale utilizza gli strumenti con diligenza e correttezza, in modo da non causare danni o pericoli ai beni, ai dati e alle informazioni trattate, nel rispetto dei doveri propri del pubblico dipendente di cui al D.P.R. 62/2013 e al codice di comportamento dell'Istituto. In particolare il personale: custodisce gli strumenti in modo appropriato; li impiega per le sole finalità connesse al rapporto di servizio; segnala tempestivamente furto, danneggiamento o malfunzionamento.

Ai sensi dell'art. 11-bis, comma 4, del D.P.R. 62/2013, è consentito l'utilizzo degli strumenti informatici forniti dall'Istituzione scolastica per incombenze personali, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali, per la sicurezza e per il corretto funzionamento delle risorse. L'utilizzo per finalità istituzionali di strumenti personali del dipendente è consentito solo previa autorizzazione e valutazione di sicurezza, secondo l'art. 12, comma 3-bis, del CAD.

5. Autenticazione e gestione delle credenziali

Tutti gli utenti che accedono alla rete e alle risorse informatiche dell'Istituto devono essere univocamente identificabili (Misure minime AgID, ABSC 1 e ABSC 5). L'accesso ai servizi avviene secondo il profilo di autorizzazione assegnato; i privilegi di amministratore sono riservati ai soli soggetti formalmente incaricati.

Le credenziali (User ID e password) sono **strettamente personali** e non devono essere divulgate: ogni operazione effettuata con le credenziali è attribuita al soggetto titolare delle stesse. Ove disponibile, l'accesso è protetto con **autenticazione a più fattori (MFA)**; l'accesso ai servizi on line dell'Istituto dovrà avvenire tramite SPID o CIE. In caso di sospetta compromissione delle credenziali, l'utente avverte immediatamente l'amministratore di sistema, che attiva le verifiche e il reset.

La password deve essere robusta e non facilmente ricostruibile. Si raccomanda di:

- NON utilizzare: la User ID, il proprio nome/cognome o dati personali (data di nascita, codice fiscale, ecc.), nomi di familiari o personaggi noti, parole di senso compiuto, sequenze banali (123456, qwerty), sigle dell'ufficio o dell'applicativo;
- USARE: stringhe lunghe che combinano lettere maiuscole e minuscole, numeri e caratteri speciali, preferibilmente sotto forma di passphrase facile da ricordare ma difficile da indovinare;
- cambiare la password al primo accesso e in caso di sospetta compromissione; non riutilizzare le credenziali di lavoro su servizi personali; non annotare le password in chiaro

né conservarle in prossimità della postazione. Per la gestione delle credenziali multiple è consigliato l'uso di un gestore di password (password manager).

Non è richiesta la consegna delle password a terzi né la loro custodia presso l'amministrazione: la riservatezza della password è responsabilità esclusiva dell'utente. La rotazione periodica obbligatoria dovrà avvenire con cadenza trimestrale.

6. Protezione della postazione e dei dispositivi

A tutela della sicurezza, il personale:

- blocca la sessione di lavoro in caso di allontanamento dalla postazione e spegne i dispositivi a fine giornata;
- non installa software non autorizzato e mantiene attivi gli aggiornamenti di sicurezza, l'antivirus/antimalware e il firewall configurati dall'amministratore di sistema;
- conserva i dati nelle aree di rete predisposte, soggette a backup; evita l'uso di supporti rimovibili non autorizzati e ne verifica l'assenza di malware;
- utilizza i dispositivi mobili (notebook, tablet, smartphone) e i dispositivi di firma digitale o CNS con la massima cura, custodendoli e proteggendoli con codici di accesso; in caso di dispositivi personali si applica l'art. 12, comma 3-bis, del CAD;
- non lascia incustoditi documenti contenenti dati personali presso le stampanti e non attiva webcam/microfoni se non per finalità istituzionali e con il consenso dei presenti, ove richiesto.

7. Utilizzo di Internet

L'accesso a Internet è fornito per finalità istituzionali. È vietato l'utilizzo che possa compromettere la sicurezza dei sistemi, ledere l'immagine dell'Amministrazione o violare la legge: in particolare l'accesso a contenuti illeciti, offensivi o discriminatori, il download di software o materiali in violazione del diritto d'autore, l'uso di servizi che espongano la rete a rischi (peer-to-peer non autorizzato, ecc.).

Il personale ha una legittima aspettativa di riservatezza, in particolare quando opera in modalità di lavoro agile. L'Istituto adotta misure tecniche e organizzative idonee a prevenire la raccolta di informazioni relative alla sfera extralavorativa e a evitare ogni forma di controllo a distanza massivo e indiscriminato, in conformità all'art. 4 dello Statuto dei lavoratori e all'art. 113 del Codice privacy.

8. Utilizzo della posta elettronica istituzionale

La casella di posta elettronica istituzionale è uno strumento di lavoro e va utilizzata per le sole finalità di servizio. Ai sensi dell'art. 11-bis del D.P.R. 62/2013, ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e indicare un recapito istituzionale; il personale si uniforma alle modalità di firma dei messaggi individuate dall'Istituto ed è responsabile del contenuto dei messaggi inviati.

È vietato l'invio, all'interno o all'esterno dell'Amministrazione, di messaggi oltraggiosi, discriminatori o comunque idonei a determinare responsabilità per l'Istituzione scolastica (art. 11-bis, comma 5, D.P.R. 62/2013). Non è consentito l'uso di caselle di posta personali per lo svolgimento di attività istituzionali.

In caso di assenza programmata, il personale attiva un messaggio di risposta automatica con l'indicazione di un recapito alternativo. La continuità delle comunicazioni in caso di assenza prolungata o cessazione è assicurata mediante caselle di gruppo/funzionali e deleghe organizzative, evitando l'accesso indiscriminato alla corrispondenza individuale; alla cessazione del rapporto la casella nominativa è disattivata, previo congruo periodo di risposta automatica che informa i terzi del nuovo recapito.

9. Utilizzo dei social media

Ai sensi dell'art. 11-ter del D.P.R. 62/2013, nell'utilizzo dei propri account personali di social media il dipendente adotta ogni cautela affinché le proprie opinioni o i propri giudizi non siano in alcun modo attribuibili direttamente all'Istituzione scolastica o alla pubblica amministrazione. Il personale si astiene da interventi o commenti che possano nuocere al prestigio, al decoro o all'immagine dell'Amministrazione di appartenenza o della pubblica amministrazione in generale. La gestione dei canali social istituzionali è riservata ai soggetti espressamente autorizzati.

10. Trattamento dei metadati di posta, log e controlli

L'Istituto, tramite l'amministratore di sistema, può trattare i soli metadati e log necessari ad assicurare il funzionamento e la sicurezza delle infrastrutture informatiche. In conformità al Provvedimento del Garante del 6 giugno 2024, n. 364, i **metadati di posta elettronica** (dati esterni di invio/ricezione e smistamento, distinti dal contenuto dei messaggi, che resta nella disponibilità dell'utente) sono conservati per un periodo limitato a pochi giorni e, in via orientativa, **non superiore a 21 giorni**; una conservazione più estesa è ammessa solo in presenza di specifiche e comprovate esigenze tecniche o di sicurezza, in accountability e con le garanzie dell'art. 4, comma 1, dello Statuto dei lavoratori.

I log di sistema e di navigazione sono raccolti in forma minimizzata, conservati per il tempo strettamente necessario e protetti da accessi non autorizzati. I controlli sono effettuati in modo graduale, non massivo e non continuativo, nel rispetto dell'art. 4 dello Statuto dei lavoratori, dei principi di liceità, minimizzazione e limitazione della conservazione, e previa idonea informativa; ove necessario è svolta una valutazione d'impatto (DPIA). L'eventuale accesso alla corrispondenza individuale avviene solo in casi eccezionali, documentati e con il coinvolgimento del DPO. L'amministratore di sistema opera secondo il Provvedimento del Garante del 27 novembre 2008 in materia di amministratori di sistema.

11. Sicurezza, gestione degli incidenti e violazioni dei dati

L'Istituzione scolastica adotta le Misure minime di sicurezza ICT di AgID e tiene conto della cornice introdotta dalla Legge 90/2024 e dal D.Lgs. 138/2024 (NIS2) in materia di cybersicurezza. Il personale che rilevi un incidente di sicurezza, un sospetto accesso abusivo (art. 615-ter c.p.), un malware o un'anomalia, ne dà immediata comunicazione all'amministratore di sistema e al referente individuato dall'Istituto.

In caso di violazione di dati personali (data breach), si attiva la procedura interna prevista dagli artt. 33 e 34 del GDPR, con notifica al Garante **entro 72 ore** ove ricorrano i presupposti e comunicazione agli interessati nei casi di rischio elevato. Per gli incidenti informatici rilevanti, l'Istituto effettua le ulteriori segnalazioni eventualmente dovute all'Agenzia per la Cybersicurezza Nazionale (ACN)/CSIRT Italia secondo il perimetro di applicazione e le tempistiche di legge (24/72 ore).

12. Cessazione del rapporto, riassegnazione e smaltimento dei supporti

Alla cessazione o variazione del rapporto di servizio, l'amministratore di sistema disabilita le utenze e revoca le autorizzazioni; il personale restituisce gli strumenti assegnati. Prima della riassegnazione o dismissione dei dispositivi e dei supporti di memorizzazione, i dati sono cancellati in modo sicuro e irreversibile; lo smaltimento avviene nel rispetto della normativa sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE) e delle misure di sicurezza dei dati personali.

13. Formazione

L'Istituzione scolastica promuove la formazione e la sensibilizzazione del personale sull'uso sicuro degli strumenti informatici, sulla protezione dei dati personali e sul riconoscimento delle minacce (phishing, social engineering, ransomware), anche in attuazione degli obblighi formativi in materia di tecnologie informatiche e di cybersicurezza. La conoscenza del presente Disciplinare è parte integrante di tale percorso.

- Controlli e sanzioni

Il rispetto del presente Disciplinare è oggetto di verifica nel rispetto dei principi sopra richiamati. La violazione delle disposizioni può integrare illecito disciplinare e dar luogo ai relativi procedimenti secondo il CCNL del Comparto Istruzione e Ricerca, il D.Lgs. 165/2001, il D.P.R. 62/2013 e il codice di comportamento, fatte salve le eventuali responsabilità civili, contabili e penali. Le sanzioni sono applicate secondo criteri di gradualità e proporzionalità, garantendo il contraddittorio.

Si ricorda che ex DPR n. 81/2023, art. 11 (Codice di Comportamento dei dipendenti pubblici)

1. Art. 11-ter (Utilizzo dei mezzi di informazione e dei social media). - 1. Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinchè le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla pubblica amministrazione di appartenenza.

2. In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.

- Disposizioni finali

Il presente Disciplinare entra in vigore dalla data di adozione ed è portato a conoscenza di tutto il personale mediante pubblicazione sul sito istituzionale. Esso integra l'informativa resa ai sensi dell'art. 13 del GDPR. Per quanto non espressamente previsto si rinvia alla normativa vigente; eventuali modifiche o integrazioni sono adottate con le medesime modalità del presente atto e prevalgono sulle disposizioni incompatibili.

Il Dirigente Scolastico
Prof.ssa Laura Maria Cestaro
Firma autografa sostituita a mezzo stampa
ai sensi dell'art.3 comma 2 del D.Lgs n.39/1993