ISTITUTO OMNICOMPRENSIVO "Dante Alighieri"
Via Septempedana, s.n.c. - 06025 NOCERA UMBRA (PG)
Tel. 0742/818860 - 0742/818701
e-mail: pgic82800p@istruzione.it - **pec:** pgic82800p@pec.istruzione.it
www.scuolenoceraumbra.edu.it - **C.F. 83004080541**
Ministero dell'Istruzione Università e Ricerca
We prepare for Cambridge English Qualifications

Prot. N. *(ved.segnatura)*
Circ. N. *(ved.segnatura)*

All'Ufficio tecnico
All'A.D. della scuola
A tutti i docenti
A tutto il personale ATA – SEDE

All'Albo pretorio
Ad Ammne trasparente

OGGETTO: privacy e sicurezza informatica a scuola

Facendo seguito alla formazione in oggetto erogata in data 24/9/2025, si inviano in allegato:
- il Vademecum del Garante del 2023, in linea con il Reg.UE 679/16 GDPR e inerente la privacy a scuola
- il Vademecum dell'Agenzia per la Cybersicurezza (ACN), riferito alla sicurezza informatica

PRIVACY A SCUOLA

Si sottolinea che tutte le scuole possono trattare i **dati personali degli studenti**, anche relativi a *categorie particolari* (es: origine razziale, fede religiosa, stato di salute…), se funzionali all'attività didattico-formativa, per perseguire specifiche finalità istituzionali o se espressamente previsto dalla normativa di settore (es: per l'inclusione, la gestione assenze per malattia, l'istruzione domiciliare, le allergie/intollenze…).
Il consenso scritto esplicito, invece, va usato per attività non strettamente connesse a quelle didattiche.

In relazione alla **vita dello studente** si forniscono le seguenti indicazioni (esemplificative, non esaustive):
- all'*iscrizione*, non è possibile chiedere informazioni aggiuntive che esulano dai fini istituzionali (ad es., non è richiedibile lo stato di famiglia, né la professione dei genitori)
- la diffusione dei dati relativi alla *composizione delle classi prime* sul sito web istituzionale non è consentita: di prassi è consentita la pubblicazione dei soli nominativi (es: senza residenza, luogo/data di nascita…) in un tabellone esposto nella bacheca scolastica
- nei *temi* scritti, è possibile assegnare temi riguardanti il mondo personale o familiare ma la cautela va osservata nell'eventuale lettura dello stesso in classe: il focus primario è sulla salvaguardia del minore evitando conseguenze, anche relazionali, che potrebbero derivare dalla conoscibilità di informazioni personali o vicende familiari tra i compagni di classe
- quanto agli *studenti con BES*, non è consentito inviare comunicazioni aperte o pubblicare online circolari con nomi degli studenti BES coinvolti nella specifica attività, limitando la conoscenza ai soli soggetti legittimati (es: docenti, genitori, operatori sanitari) che devono predisporre il PEI/PDP
- non si può pubblicare sul sito della scuola o inserire in bacheca, i nomi degli alunni i cui genitori sono in ritardo nel *pagamento della mensa*: in generale, gli avvisi devono avere sempre un carattere generale, mentre alle singole persone ci si deve rivolgere con comunicazioni di carattere individuale
- analogamente, non sono pubblicabili le liste di alunni che usufruiscono di uno specifico *servizio scuolabus*, in quanto tale diffusione di dati può rendere i minori facile preda di eventuali malintenzionati
- il *registro elettronico* deve essere usato con attenzione per prevenire che, ad es., informazioni personali/delicate relative a singoli studenti/docenti siano messe a disposizione di terzi o altro personale non autorizzato
- agli *scrutini*, fatto salvo lo specifico regime di pubblicità relativo agli esiti degli Esami di Stato, non è ammessa la pubblicazione online degli esiti degli scrutini. Quindi, gli esiti degli scrutini intermedi/finali e di ammissione agli Esami di Stato vanno resi disponibili, con la sola indicazione "*ammesso"* o *"non ammesso*" nell'area riservata del Registro elettronico cui possono accedere solo gli studenti della classe

- la *diffusione a enti/privati* degli esiti formativi degli studenti (es: voto di diploma) e loro altri dati personali (es: mail, indirizzo…), allo scopo di favorirne l'inserimento nel mercato del lavoro o all'Università, può esser fatta, su richiesta degli studenti interessati, previa idonea informativa

In relazione ai **social e alle nuove tecnologie**, il documento precisa che:

- bisogna rendere consapevoli che le proprie azioni in Rete possono produrre *effetti negativi* anche nella vita reale e per un tempo indefinito, prestando attenzione a *comportamenti anomali* (derivanti da *bullismo, revenge porn, sexting*, ecc…)
- è bene informare anche genitori/tutori che anch'essi devono prestare particolare attenzione se intendono condividere online *contenuti che riguardano i figli* (es: foto, video, ecografie, ecc..);
- nelle *recite/saggi*, ecc…, le riprese video e le foto fatte dai genitori durante le tali manifestazioni non violano la privacy qualora raccolte per fini personali e destinate all'ambito familiare, mentre invece la loro diffusione/pubblicazione su Internet o social è illecita poiché richiede il consenso degli altri soggetti coinvolti/ripresi
- le scuole che utilizzano sistemi di *didattica a distanza* nell'ambito delle proprie finalità istituzionali non devono chiedere il consenso al trattamento dei dati di studenti, genitori e docenti: se la piattaforma prescelta per l'erogazione dell'attività didattica a distanza comporta il trattamento di dati personali di studenti, genitori, docenti o altro personale per conto della scuola, il rapporto con il fornitore dovrà essere regolato con un contratto e le scuole dovranno assicurarsi che i dati trattati per loro conto siano utilizzati solo per finalità didattiche; non è invece ammessa la videoregistrazione della lezione in cui si manifestano le c.d. *dinamiche di classe*, neanche qualora si utilizzino piattaforme per la didattica a distanza, in quanto possono ragionevolmente coinvolgere studenti BES, con fragilità, ecc…
- è possibile la *registrazione della lezione* esclusivamente per scopi personali per alunni DSA certificati in base ai loro PDP, mentre la diffusione è illecita e richiede il preventivo consenso delle persone coinvolte nella registrazione (docenti, famiglie, studenti, altro personale…)

In relazione alla **videosorveglianza**, è possibile installare un sistema di videosorveglianza nelle scuole, quando indispensabile per tutelare l'edificio e i beni scolastici, circoscrivendo le riprese alle aree interessate, come ad es. quelle soggette a furti/atti vandalici, attivandole, all'interno dell'istituto, al termine delle attività scolastiche/extrascolastiche. Di contro, le aree perimetrali esterne degli edifici scolastici possono essere oggetto di ripresa, segnalata da appositi cartelli, per tutelare l'edificio e i beni, anche in orario di apertura degli stessi.

La raccolta di informazioni personali, spesso anche appartenenti a particolari categorie di dati, per **attività statistica e di ricerca** effettuata da soggetti legittimati ed esterni alla scuola attraverso questionari, è consentita solo se i ragazzi (o i genitori, nel caso di minori) sono stati preventivamente informati in merito alle caratteristiche essenziali del trattamento dei loro dati personali, pur restando sempre liberi di non aderire all'iniziativa.

Infine, si ricorda che le Scuole trattano lecitamente **dati dei dipendenti docenti/Ata** per instaurazione/cessazione del rapporto di lavoro, gestione assenze, obblighi di comunicazione alle autorità di previdenza e assicurazione, ecc… La stessa pubblicazione in Albo online di *graduatorie, circolari, determinazioni*, ecc.. deve avvenire nel rispetto dei principi generali di protezione dei dati, che devono essere "adeguati, pertinenti e limitati" rispetto alle finalità istituzionali perseguite dalla scuola. Le scuole possono, inoltre, pubblicare *graduatorie per supplenze* di docenti e Ata, con solo i dati strettamente necessari all'individuazione del candidato, come il nome, il cognome, il punteggio e la posizione in graduatoria (evitando, quindi, recapiti e indirizzi privati).

SICUREZZA INFORMATICA

Si invia in allegato il Vademecum dell'Agenzia per la Cybersicurezza Nazionale (ACN) intitolato "*Buone pratiche di cybersecurity di base per i dipendenti delle PP.AA*.", con linee guida sulla *cyber hygiene* per i dipendenti pubblici in un contesto in rapido mutamento dove è cruciale promuovere ambienti digitali sicuri per cittadini, Enti ed imprese.

Tra le **misure suggerite** nel documento:

- uso di password sicure, da cambiare spesso, abbinate ad altri sistemi di accesso (es: password e OTP, password e codice d'accesso via SMS)
- aggiornamenti di antivirus
- uso di software scelti dalla P.A. e accesso in piattaforme relative alle sole attività lavorative
- non collegarsi, con i dispositivi di lavoro, in reti Wi-fi pubbliche non protette
- non fidarsi di email sospette, che chiedono di agire urgentemente, dove si chiede di cliccare un particolare sito, ecc…
- non inserire MAI contenuti sensibili in siti di Intelligenza Artificiale o chatbot

In caso di **dubbi** su possibili frodi, comportamenti giusti / erronei, consigli di cybersicurezza, ecc…, si prega di rivolgersi preliminarmente all'Ufficio tecnico o all'Animatore digitale della scuola.

Si rimanda all'attenta lettura delle guide allegate.
Distinti saluti.

Nocera Umbra, li (ved.segnatura).

Il Dirigente Scolastico
Prof. Leano Garofoletti
(Firmato digitalmente ai sensi del D.Lgs 82/05 CAD e ss.mm.ii.)