



ISTITUTO COMPRENSIVO EX "S.M. PASCOLI"

Via Parini, 1 - 75100 MATERA

Cod. Ministeriale: MTIC82700A / E-mail: mtic82700a@istruzione.it / Pec: mtic82700a@pec.istruzione.it

C.F.: 93051600778 / Sito: www.icpascolimatera.it / Telefono: 0835.386254

**LINEE GUIDA IN TEMA DI PRIVACY E SICUREZZA INFORMATICA
PER IL TRATTAMENTO DI DATI PERSONALI EFFETTUATO AL DI FUORI DELLA SEDE DI LAVORO E/O
MEDIANTE LE MODALITÀ DI SVOLGIMENTO AGILE DELLA PRESTAZIONE LAVORATIVA**

Le presenti linee guida forniscono le indicazioni operative per il trattamento di dati personali effettuato al di fuori della sede di lavoro e/o mediante le modalità di svolgimento agile della prestazione lavorativa e costituiscono parte integrante delle istruzioni impartite alle persone autorizzate al trattamento ai sensi dell'art. 29 del Regolamento UE 2016/679 e dell'art. 2-quaterdecies del D. Lgs. 196/2003. Le prescrizioni sono finalizzate a garantire un livello di protezione adeguato delle dotazioni tecnologiche utilizzate e il rispetto dei principi di integrità, riservatezza e disponibilità dei dati e delle informazioni, riducendo al minimo i rischi di accesso non autorizzato, trattamento non consentito o non conforme alle finalità, distruzione o perdita dei dati.

Principali prescrizioni

1. Proteggere l'accesso alla rete e alle dotazioni tecnologiche (PC, notebook, tablet, smartphone, ecc.) mediante credenziali personali, robuste e diverse per i diversi servizi. Ove disponibile, deve essere attivata l'autenticazione a più fattori (MFA). Le credenziali non devono essere condivise con terzi né riutilizzate per servizi diversi; eventuali password temporanee devono essere modificate al primo accesso.
2. Utilizzare esclusivamente dispositivi dotati di sistemi operativi e software autentici, supportati dal produttore e costantemente aggiornati. Gli aggiornamenti di sicurezza devono essere installati con regolarità; non è consentito trattare dati personali mediante dispositivi con sistemi operativi non più supportati o privi degli aggiornamenti di sicurezza.
3. Nel caso di utilizzo di un dispositivo condiviso, deve essere utilizzato un account personale e riservato, protetto da credenziali proprie. L'accesso ai dati e ai servizi istituzionali non deve avvenire mediante account del sistema operativo condivisi con altri utilizzatori del dispositivo.
4. Garantire che sul dispositivo siano attivi e aggiornati gli strumenti di protezione messi a disposizione dal sistema operativo o dall'Istituzione scolastica, con particolare riferimento a firewall, protezione antimalware/antivirus e aggiornamenti automatici di sicurezza. Tali strumenti non devono essere disattivati o alterati senza autorizzazione.
5. Le password non devono essere memorizzate in chiaro, annotate in luoghi accessibili a terzi o salvate in modo non protetto. È consentito l'utilizzo di gestori di password affidabili e adeguatamente protetti. L'eventuale memorizzazione delle credenziali nel browser deve essere evitata sui dispositivi condivisi e, comunque, deve avvenire soltanto attraverso strumenti e configurazioni che garantiscano un adeguato livello di sicurezza.
6. La memorizzazione locale di documenti contenenti dati personali deve essere limitata ai casi

strettamente necessari e al tempo indispensabile. Deve essere privilegiato l'utilizzo dei sistemi e degli spazi di archiviazione istituzionali autorizzati. Qualora sia indispensabile conservare temporaneamente dati su un dispositivo locale o rimovibile, devono essere adottate adeguate misure di protezione, quali la cifratura del dispositivo o dei file, e i dati devono essere cancellati in modo sicuro non appena cessata la necessità del trattamento.

¹La password deve essere sufficientemente lunga e complessa, ad esempio deve essere composta da almeno 8 caratteri, contenere almeno un carattere appartenente alle lettere maiuscole e almeno un carattere appartenente alle lettere minuscole, contenere almeno un carattere appartenente alle 10 cifre (0-9), contenere almeno un carattere appartenente ai caratteri non alfabetici (ad esempio !,\$,#,%), essere diversa dall'ultima utilizzata e mai riconducibile alla propria sfera personale o professionale.

Matera, 07/09/2026

LA DIRIGENTE REGGENTE
Prof.ssa Marialuisa Sabino

Documento informatico firmato digitalmente ai sensi del D. Leg.vo n. 82/2005 e norme collegate

7. Anche al di fuori della sede di lavoro devono essere adottate misure organizzative idonee a garantire la riservatezza delle informazioni: evitare che terzi, compresi i familiari, possano visualizzare documenti o schermate, non lasciare incustoditi i dispositivi, bloccare la sessione in caso di allontanamento e custodire con cura eventuale documentazione cartacea.
8. L'eventuale accesso da remoto ai sistemi o alle risorse informatiche dell'Istituzione scolastica è consentito esclusivamente mediante strumenti, servizi e modalità preventivamente autorizzati dall'Istituzione e configurati in modo da garantire adeguati livelli di sicurezza, autenticazione e cifratura delle comunicazioni. Non è consentito installare o utilizzare autonomamente software di accesso remoto non autorizzato.