



ISTITUTO COMPRENSIVO STATALE CASARANO POLO 3 “Galileo Galilei”

Piazza San Domenico - 73042 CASARANO (LE)

Tel. 0833/332031 e-mail: leic861002@istruzione.it PEC: leic861002@pec.istruzione.it

www.polo3casarano.edu.it C.F. 90018430752 – Cod. MIUR: LEIC861002

LINEE GUIDA IN MATERIA DI SICUREZZA PER IL PERSONALE AMMINISTRATIVO INCARICATO DEL TRATTAMENTO DEI DATI PER IL CONTRASTO E IL CONTENIMENTO DELL'EMERGENZA COVID – 19

Vengono di seguito riportate le norme cui dovrà attenersi il personale incaricato del trattamento dei dati personali utili al fine di adottare misure per il contenimento e il contrasto del virus Covid – 19.

Per chiarezza, si ricorda che i dati che l'istituto può raccogliere a tal fine sono:

- 1) nome, cognome, telefono, data, ora di ingresso, ora di uscita dei visitatori;
- 2) la rilevazione in tempo reale della temperatura corporea dell'allievo o del personale scolastico o di colui che, a qualsiasi titolo, debba accedere all'interno dell'edificio scolastico o nelle sue pertinenze, ovvero, le informazioni riguardanti l'assenza condizioni di salute che impediscono l'accesso ai locali (tipo ontomatologia respiratoria o temperatura corporea superiore a 37,5°);
- 3) le informazioni in merito a contatti stretti ad alto rischio di esposizione, negli ultimi 14 giorni, con soggetti sospetti o risultati positivi al COVID-19;
- 4) le informazioni in merito alla provenienza, negli ultimi 14 giorni, da zone a rischio secondo le indicazioni dell'OMS.
- 5) la certificazione medica da cui risulti la “avvenuta negativizzazione” del tampone secondo le modalità previste e rilasciata dal dipartimento di prevenzione territoriale di competenza; 6) situazioni di particolare fragilità e patologie attuali o pregresse dei dipendenti o alunni.

Ulteriori informazioni sulla modalità del trattamento dei dati e sulle misure di sicurezza adottate sono contenute nel registro dei trattamenti.

In sede di registrazione del dato della temperatura corporea, registrare la sola circostanza del superamento della soglia stabilita dalla legge e comunque quando è necessario documentare le ragioni che hanno impedito l'accesso;

Assicurare modalità tali da garantire la riservatezza e la dignità dell'interessato in caso di isolamento momentaneo, dovuto al superamento della temperatura;

Acquisire i dati nel rispetto della dignità dell'interessato, avendo cura di tenere nascosto il contenuto a terzi non autorizzati al trattamento;

Controllare e custodire immediatamente gli atti e i documenti contenenti dati personali in modo da assicurarne l'integrità e la riservatezza;

Conservare sempre i dati del cui trattamento si è incaricati in apposito armadio assegnato;

Accertarsi della corretta funzionalità dei meccanismi di chiusura dell'armadio, segnalando tempestivamente eventuali anomalie;

Prima di procedere alla raccolta e al trattamento dei dati fornire sempre l'informativa all'interessato o alla persona presso cui si raccolgono i dati;

Occorre procedere alla raccolta dei dati con la massima cura verificando l'esattezza dei dati stessi;

Si può accedere ai soli dati personali, oggetto di trattamento, la cui conoscenza sia strettamente necessaria per lo svolgimento delle funzioni e dei compiti affidati e per le finalità di cui al provvedimento di incarico;

I documenti o atti che contengono dati sensibili o giudiziari devono essere conservati in archivi (ad esempio stanze, armadi, schedari, contenitori in genere) chiusi a chiave;

Non fornire telefonicamente o a mezzo fax dati e informazioni relativi a terzi, senza una specifica autorizzazione del titolare;

Qualora giungano richieste telefoniche di dati sensibili da parte dell'Autorità sanitaria, di quella giudiziaria o degli organi di polizia si deve richiedere l'identità del chiamante. Quindi si provvederà a richiamare avendo così la certezza sull'identità del richiedente;

Non fornire, anche telefonicamente o per mail, dati e informazioni ai diretti interessati senza avere la certezza della loro identità;

Nella comunicazione di dati sensibili adottare sempre procedure che permettano di garantire la sicurezza e la riservatezza delle informazioni anche mediante tecniche di anonimizzazione e di pseudonimizzazione;

I documenti cartacei non più utilizzati, specie se sensibili, devono essere distrutti o comunque resi illeggibili, prima di essere eliminati o cestinati;

Non consentire l'accesso alle aree in cui sono conservati dati personali su supporto cartaceo a estranei e a soggetti non autorizzati;

Conservare i documenti ricevuti da genitori/studenti o dal personale in apposite cartelline non trasparenti;

Consegnare al personale o ai genitori/studenti documentazione inserita in buste non trasparenti;

Non consentire l'accesso a estranei ad aree in cui sono custoditi documenti cartacei o contengano supporti informatici di memorizzazione;

Non abbandonare la postazione di lavoro per la pausa o altro motivo senza aver provveduto a custodire in luogo sicuro i documenti trattati;

Segnalare tempestivamente al Responsabile la presenza di documenti incustoditi provvedendo temporaneamente alla loro custodia;

Attenersi alle direttive ricevute e non effettuare operazioni per le quali non si è stati espressamente autorizzati dal Titolare.

Riguardo ai trattamenti eseguiti con supporto informatico attenersi scrupolosamente alle seguenti

indicazioni:

Per l'accesso al sistema informatico utilizzare le credenziali di accesso ricevute;

Adottare le necessarie cautele per assicurare la segretezza della parola chiave e la diligente custodia di ogni altro dispositivo di autenticazione informatica (badge, schede magnetiche, chiavi USB, etc.);

È fatto divieto comunicare a qualunque altro incaricato le proprie credenziali di accesso al sistema informatico;

La parola chiave deve essere modificata almeno ogni tre mesi;

La parola chiave deve essere chiusa in una busta opaca, sigillata e controfirmata sui lembi, da consegnare all'Incaricato della custodia delle copie delle credenziali, che ne curerà la conservazione;

In caso di necessità il titolare o l'Incaricato della custodia delle copie delle credenziali hanno la possibilità, previa comunicazione all'incaricato, di aprire la busta, per esigenze operative o di organizzazione.

L'incaricato nel tal caso provvederà a sostituire la parola chiave violata;

Tutte le volte che si abbandoni la propria postazione di lavoro i pc e/o i terminali devono essere posti in condizione di non essere utilizzati da estranei. In particolare si raccomanda di chiudere tutte le applicazioni in uso e di porre un blocco del sistema mediante password;

Spegnere sempre il PC alla fine della giornata lavorativa o in caso di assenze prolungate dalla postazione di lavoro;

Qualora si dovessero riscontrare difformità dei dati trattati o nel funzionamento degli elaboratori occorre darne immediata comunicazione al titolare del trattamento;

Utilizzare l'antivirus per la verifica di ogni documento trattato o di qualunque file scaricato da Internet;
Utilizzare sempre l'antivirus per verificare il contenuto di qualunque supporto di memorizzazione sospetto;
Aggiornare con frequenza l'antivirus.

Utilizzare esclusivamente le piattaforme identificate dalla scuola come sicure e nominate dalla stessa responsabili del trattamento, specie qualora si renda necessario effettuare delle attività lavorative a distanza, come previsto dalle modalità organizzative della scuola e dalla normativa vigente;

Verificare sempre la corretta modifica e/o cancellazione di dati su documenti, cartelle o informazioni condivise alle quali si abbia accesso nell'esercizio delle proprie funzioni (double check), al fine di evitare modifiche o cancellazioni indesiderate che possano arrecare danno agli interessati o limitare le possibilità di lavoro di colleghi.

Regole per la scelta delle parole chiave

Usare una parola chiave di almeno otto caratteri;

La parola chiave non deve contenere riferimenti facilmente riconducibili all'incaricato (come per esempio nome, cognome, data di nascita, numeri di telefono, etc. propri o dei propri familiari);

Usare una combinazione di caratteri alfabetici e numerici, meglio se contenente almeno un segno di interpunzione o un carattere speciale;

Conservare con cura la parola chiave evitando di trascriverla su fogli posti in vista in prossimità del PC o sulla rubrica dell'ufficio.

Si precisa che il titolare è sempre e comunque responsabile della mancata esecuzione degli adempimenti previsti dal D.lgs. n.196/2003 e del Regolamento UE 2016/679. Tuttavia le responsabilità, per l'inosservanza delle istruzioni impartite dal Titolare e/o dai responsabili, possono riguardare anche gli incaricati, che non rispettino o non adottino le misure necessarie.



LA DIRIGENTE SCOLASTICA
(Prof.ssa Rita Augusta PRIMICERI)
Rita Augusta