Ministero dell'Istruzione, dell' Università e della Ricerca
Ufficio Scolastico Regionale per il Lazio
Istituto di Istruzione Superiore
"Apicio – Colonna Gatti"
Sede Legale via Gramsci, 110
Sede Amministrativa: Via Nerone, 1 – 00042 Anzio (RM)
TEL. **0698610038** – e-mail: **rmis12200t@istruzione.it** - e-mail PEC: **rmis12200t@pec.istruzione.it**
Sito web: **www.iis-apicio-colonnagatti.edu.it**
C.M.: **RMIS12200T** - C.F.: **96419030588**

con sezioni associate di:
IPSSEOA "Apicio" Anzio Via Nerone 1 - 00042 Anzio (RM) Tel. 0698610038 - Via delle Bouganvillae, 7 - 00042 Lavinio (RM) – **Corso Serale RMRH12250A** Tel. 06121128145 – C.M.: RMRH122012
IP "Colonna Gatti" Anzio Via Filibeck, 2 - 00042 Anzio (RM) - Tel. 06121128485
Corso ordinario: C.M.: RMRC12201R – Corso serale: C.M.: RMRC122516
Via Orsenigo, 1 – 00048 Nettuno (RM) -Tel 06121128505 – C.M.: RMRC12202T

Atto di Nomina dell'operatore scolastico – utente del sistema ReCUP - Scuola ad "*incarico del trattamento dei dati personali*" in osservanza della normativa nazionale ed europea in materia di Protezione dei dati personali .

VISTO

Il decreto legislativo 30 giugno 2003, n. 196 c.d. "Codice in materia di protezione dei dati personali", come modificato dal decreto legislativo 10 Agosto 2018, n. 101.

Il Regolamento dell'Unione Europea n. 679/2016.
ed in particolare:
- L'art 4 paragrafo 7 Regolamento UE 679/2016 che definisce il Titolare del trattamento come la persona fisica, la persona giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

- l'art 4 paragrafo 8 Regolamento UE 679/2016 che definisce il Responsabile del trattamento come la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

- Il combinato disposto articoli 4 parag. 10 e 29 del Regolamento UE 679/2016 che individuano la figura degli autorizzati al trattamento sotto l'autorità diretta del Titolare e/o del Responsabile del trattamento, ossia coloro

che devono essere istruiti in tal senso (figura riconducibile a quella dell'incaricato del trattamento prevista dalla previgente normativa nazionale sulla Privacy)

CONSIDERATO

- Che, in attuazione della campagna scuola, gli operatori scolastici - preposti alla gestione delle prenotazioni degli esami COVID 19 per i docenti - dovranno trattare i dati personali dei docenti stessi.

- Che i dati personali dei suddetti docenti rientrano nella sfera di Titolarità della struttura scolastica di appartenenza ai sensi di legge.

- Che la suddetta attività di gestione delle prenotazioni di esami COVID 19, comportando un trattamento costante di dati/informazioni personali, rientra nell'ambito di applicazione della normativa in materia di protezione dei dati personali (privacy). Pertanto, in osservanza della citata normativa, risulta necessario designare il personale che tratta i predetti dati, quale incaricato del trattamento, autorizzando lo stesso all'effettuazione delle relative operazioni e fornendo le istruzioni di seguito riportate, con particolare riferimento agli obblighi inerenti la riservatezza.

RITENUTO

Pertanto, di dover procedere alla designazione dell'operatore scolastico - che gestisce le prenotazione degli esami COVID 19 dei docenti per mezzo del sistema informativo regionale ReCUP – scuola - quale "autorizzato/incaricato del trattamento dei dati personali" in osservanza della normativa in materia di protezione dei dati personali (privacy)
Inoltre, la necessità di impartire all'operatore scolastico, designato con il presente atto, le istruzioni (riportate di seguito) relative alla corretta osservanza e attuazione della citata normativa.

NOMINA

L'Assistente Amministrativo Stefania Nieddu

INCARICATO/AUTORIZZATO DEL TRATTAMENTO

dei dati personali nell'ambito della gestione delle prenotazioni di esami COVID 19 – Campagna Recup Scuola all'interno della struttura scolastica di appartenenza.

La presente nomina è da intendersi valida solo per le tipologie di trattamento – tra quelle contemplate dall' 4 paragrafo 2) del Regolamento U.E. 679/2016 – necessarie ai fini dello svolgimento delle attività lavorative assegnate e secondo le modalità e le istruzioni riportate nel presente atto e/o impartite dal rispettivo Responsabile di Ufficio.

In particolare l'incaricato designato con il presente atto può effettuare solo quelle categorie di trattamento – ovvero operazioni o complesso di operazioni svolte sui dati con o senza l'ausilio di strumenti elettronici/automatizzati – espressamente autorizzate dal proprio Responsabile di ufficio e può accedere ai sistemi informatici/applicativi e/o data base e/o cartelle condivise e/o archivi cartacei solo previa autorizzazione dal Responsabile stesso e/o previa assegnazione di apposite credenziali di autenticazione in linea con il profilo di autorizzazione attribuito all'accesso al sistema ReCUP-scuola.

A tal fine si forniscono di seguito istruzioni e raccomandazioni in ordine alla corretta effettuazione delle operazioni di trattamento dei dati personali dei docenti scolastici che devono effettuare gli esami COVID 19 – campagna Recup Scuola in osservanza della normativa in materia di protezione dei dati personali (Privacy).

Istruzioni in ordine alle operazioni di trattamento dei dati personali

Le istruzioni di seguito riportate sono vincolanti per gli operatori scolastici se correlate all'attività lavorativa assegnata (ovvero gestione delle prenotazioni degli esami COVID 19 e attività amministrative connesse nell'ambito della struttura scolastica di appartenenza).

Le operazione di trattamento dei dati personali devono essere effettuate nel rispetto della vigente normativa nazionale ed europea in materi di trattamento dei dati personali di cui al D.Lgs. n. 196/2003, come modificato dal D.Lgs 101/2018 e al Regolamento dell'Unione Europea n. 679/2016 ovvero in osservanza delle prescrizioni e dei principi ivi contemplati (Principi di necessità, liceità, trasparenza, correttezza e proporzionalità).
Nel dettaglio.

- Il trattamento dei dati deve essere effettuato in modo lecito e corretto.
- I dati personali devono essere trattati unicamente ed esclusivamente per le finalità inerenti alle attività lavorative affidate e, quindi, devono essere raccolti, registrati e successivamente trattati unicamente per le finalità inerenti all'attività di competenza e/o attività connesse.
- Le modalità con cui si effettuano i trattamenti devono essere pertinenti e non eccedenti le finalità perseguite (ovvero l'incaricato è autorizzato al trattamento dei dati personali al solo fine di effettuare le proprie attività lavorative inerenti la gestione delle prenotazioni di esami COVID 19 nell'ambito della struttura scolastica di appartenenza) .
- Il trattamento dei dati personali deve avvenire solo se necessario allo svolgimento della propria attività lavorativa, escludendo lo stesso quando le finalità perseguite possono essere realizzate mediante l'utilizzo di dati anonimi e/o mediante modalità che permettano di identificare l'interessato solo in caso di necessità (principio di limitazione del trattamento dei dati).
- I dati personali oggetto di trattamenti devono essere raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento compatibilmente con i predetti scopi.
- Il trattamento dei dati deve essere effettuato secondo il principio di trasparenza, ovvero deve essere assicurata la consapevolezza dell'interessato in ordine al trattamento dei dati che lo riguardano.
- Se necessario e correlato alle mansioni lavorative svolte, l'incaricato deve verificare costantemente – secondo le istruzioni fornite dal proprio Responsabile – l'esattezza dei dati, il loro aggiornamento e

la loro conservazione nel rispetto delle misure/procedure di sicurezza adottate dalla struttura scolastica di appartenenza in materia di Privacy, di utilizzo degli strumenti informatici e sicurezza delle informazioni.

- L'incaricato è tenuto ad assicurarsi che i dati trattati non vadano dispersi e/o acquisiti, anche in modo incontrollato, da terzi non autorizzati al trattamento.
- Se necessario e correlato alle mansioni svolte, l'incaricato deve verificare costantemente – secondo le istruzioni fornite dal proprio Responsabile - la completezza e pertinenza dei dati trattati il cui trattamento non deve essere eccedente rispetto alle finalità per le quali sono raccolti e/o successivamente trattati.
- E' vietato modificare i trattamenti esistenti e/o introdurre nuovi trattamenti senza l'esplicita autorizzazione del proprio Responsabile.
- In caso di incidente di sicurezza che coinvolga dati personali (soprattutto dati sensibili) l'incaricato ha l'obbligo prescritto dalla legge di informare tempestivamente il Responsabile dell'Ufficio Privacy (e/o il DPO ove designato) e il Responsabile del proprio Ufficio. In particolare, si elencano a titolo esemplificativo e non esaustivo i casi di violazione dei dati personali e/o incidente di sicurezza: distruzione - accidentale e/o illecita - perdita, modifica, divulgazione e accessi non autorizzati ai dati trasmessi, conservati o comunque trattati.
- Devono essere rispettate le indicazioni e/o le istruzioni fornite dal proprio Responsabile e/o dal responsabile dell'Ufficio Privacy (e/o DPO). Le operazioni di trattamento devono essere effettuate in osservanza della normativa nazionale ed europea in materia di Privacy nonché nel rispetto delle procedure/regolamenti adottati dalla struttura scolastica di appartenenza in materia di trattamento dei dati personali (privacy), utilizzo degli strumenti informatici/elettronici e sicurezza delle informazioni
- Nel caso in cui debbano essere effettuati trattamenti - soprattutto comunicazioni/divulgazioni di dati all'esterno - l'incaricato ha l'obbligo di informare tempestivamente il proprio Responsabile al fine di ottemperare agli obblighi relativi alla normativa in materia di Privacy (es obblighi inerenti all'informativa e al consenso).
- In caso di trattamenti che esulano dall'ordinaria gestione ed esecuzione delle attività lavorative affidate (soprattutto comunicazione di dati all'interno degli uffici), l'incaricato ha l'obbligo di informare il proprio Responsabile al fine di garantire la corretta osservanza delle prescrizioni di cui alla normativa in materia di Privacy.
- Se correlato alle mansioni lavorative affidate, l'incaricato deve supportare il proprio Responsabile di Ufficio nel garantire agli interessati del trattamento l'esercizio dei diritti contemplati dal Regolamento U.E. 679/2016 nel rispetto delle procedure adottate (Diritto all'oblio, alla limitazione del trattamento, alla rettifica, all'aggiornamento, alla portabilità dei dati, di opposizione, di non subire profilazione, etc.). Al riguardo si precisa che sarà cura del Responsabile di ufficio e/o Responsabile dell'ufficio Privacy (e/o DPO) fornire ulteriori istruzioni in merito.
- Se correlato alle attività lavorative, l'incaricato deve supportare il proprio Responsabile di Ufficio nell'implementazione delle misure tecniche ed organizzative ai fini della corretta osservanza ed attuazione della normativa in materia di Privacy

- Se necessario e correlato all'attività lavorativa svolta, l'incaricato deve procedere all'eventuale cancellazione, limitazione del trattamento, pseudonimizzazione e/o cifratura dei dati nel rispetto delle istruzioni impartite dal proprio Responsabile in linea con le procedure/regolamenti adottati nonché nel rispetto delle misure di sicurezza prescritte dalla normativa in materia di Privacy.

Obblighi di riservatezza

L'incaricato del trattamento deve garantire la massima riservatezza in relazione ai dati personali trattati e/o di cui venga a conoscenza nell'espletamento delle proprie attività lavorative. L'obbligo di riservatezza deve essere rispettato anche in relazione alle credenziali di autenticazione assegnate (password) per l'accesso al sistema ReCUP – Scuola.
Nel dettaglio l'incaricato deve:

- chiedere l'autorizzazione al Responsabile di Ufficio - qualora giungano richieste anche da parte di uffici interni – per effettuare comunicazioni e/o accessi ai dati personali e/o alla documentazione che contiene i dati stessi;
- in caso di interruzione, anche temporanea, delle attività lavorative, adottare tutti gli accorgimenti ritenuti più opportuni al fine di evitare che i dati trattati non siano accessibili a terzi non autorizzati;
- raccogliere, registrare e conservare i dati presenti nei files informatici e/o nei documenti cartacei avendo cura che l'accesso agli stessi sia reso possibile solo al personale autorizzato;
- qualora giungano richieste di comunicazione di dati personali da parte dell'Autorità Giudiziaria e/o degli Organi di Polizia, avvertire comunque il proprio Responsabile di ufficio, prima di comunicare i dati stessi;
- fermo restando i divieti di cancellazione e/o obblighi di conservazione stabiliti dalle normative di legge, distruggere o comunque rendere illeggibili i documenti cartacei - che contengono dati personali - non più utilizzati, prima che gli stessi vengano cestinati.

Inoltre è vietato:

- comunicare e/o diffondere dati personali a terzi non autorizzati al trattamento senza l'autorizzazione del proprio Responsabile e/o del Responsabili dell'Area Privacy (e/o DPO) e, ove necessario, previo rilascio dell'informativa obbligatoria e/o prestazione del consenso da parte degli interessati al trattamento;
- comunicare dati personali ad un collega autorizzato al trattamento in presenza di terzi non autorizzati;
- parlare ad alta voce quando si comunicano i dati personali (anche per telefono), evitando comunque che terzi non autorizzati vengano a conoscenza di informazioni personali ascoltando la conversazione;
- comunicare ad un collega autorizzato al trattamento e/o ad un terzo non autorizzato le proprie credenziali di autenticazione.

Gli obblighi relativi alla riservatezza dei dati trattati dovranno essere osservati anche a seguito di cambiamento delle mansioni lavorative assegnate (es. mobilità), cessazione del rapporto di lavoro e/o temporanea sospensione delle attività lavorative (es. aspettativa, maternità e/o congedi parentali).

***

Il trattamento dei dati deve avvenire assicurando la tutela della riservatezza, integrità e disponibilità dei dati stessi, nonché nel rispetto della dignità della persona dell'interessato al trattamento. In particolare le operazioni di trattamento devono essere effettuate eliminando ogni occasione di impropria e/o illegittima conoscibilità di informazioni personali da parte di terzi non autorizzati al trattamento.

Qualora il trattamento dei dati sia effettuato in violazione dei principi sopra menzionati e di quanto disposto dalla normativa in materia di Privacy, **l'incaricato ha l'obbligo stabilito dalla normativa stessa di informare tempestivamente il proprio Responsabile di Ufficio** al fine di procedere eventualmente al blocco dei dati trattati (vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del trattamento medesimo) e/o consentire l'osservanza degli obblighi di legge relativi alle notifiche al Garante Privacy (data breach).

Obblighi inerenti al trattamento con l'ausilio di strumenti elettronici

Le istruzioni di seguito riportate sono vincolanti per l'operatore scolastico solo se correlate all'attività lavorativa assegnata.

In base a quanto stabilito dalla normativa vigente in materia di protezione dei dati personali, per le operazioni di trattamento dei dati personali effettuate con strumenti elettronici/automatizzati, l'incaricato del trattamento deve osservare – ove ricorrano i presupposti - le misure di sicurezza adottate dalla struttura scolastica di appartenenza e specificate nei relativi regolamenti e/o procedure in materia di Privacy, in materia di utilizzo di strumenti informatici, internet e posta elettronica.

Nel dettaglio si riportano di seguito gli obblighi inerenti all'utilizzo delle credenziali di autenticazione (UserID e Password).

L'incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata delle proprie credenziali di autenticazione (con particolare riferimento alle credenziali di accesso al Sistema ReCUP- Scuola) nonché la diligente custodia dei dispositivi elettronici (computer) in uso esclusivo e/o comunque in possesso dell'incaricato.
Nel dettaglio risulta necessario:

- Elaborare la password secondo le indicazioni fornite e conservare la segretezza sulla stessa e sulle altre componenti riservate della credenziale di autenticazione (username).
- Rispettare i profili di autorizzazione attribuiti ai fini dell'accesso ai dati e ai sistemi (ovvero all'utilizzo di determinati applicativi informatici e/o piattaforme informatiche nell'ambito delle attività lavorative assegnate).

- Custodire in modo diligente i dispositivi elettronici in possesso e/o in uso esclusivo.

Inoltre, si precisa quanto segue:

- La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri, di cui almeno quatto devono essere di natura numerica.
- Risulta necessario che la parola chiave non contenga riferimenti agevolmente riconducibili all'incaricato; quindi, la parola chiave non deve essere: il nome o il cognome dell'incaricato, il soprannome, la data di nascita propria, dei figli o degli amici, il nome di un hobby o di una passione conosciuta o facilmente conoscibile dai colleghi, il nome e cognome di personaggi famosi, etc.

E' vietato:

- rivelare la parola chiave a terzi non autorizzati;
- scrivere la parola chiave in un messaggio di posta elettronica;
- rivelare la parola chiave al superiore;
- dare indicazione in merito al formato ed alla lunghezza della parola chiave;
- svelare la parola chiave su questionari e/o su formulari di sicurezza.

La parola chiave deve essere modificata dall'incaricato almeno ogni sei mesi, in caso di trattamento di dati sensibili e/o di dati giudiziari la parola chiave deve essere modificata obbligatoriamente ogni tre mesi. Al riguardo si precisa che il sistema ReCUP gestito da LAZIOcrea prevede in automatico la modifica della parola chiave ogni tre mesi.

Si riportano di seguito ulteriori istruzioni in ordine all'utilizzo di strumenti elettronici.

- ✓ L'incaricato ha l'obbligo di terminare la sessione di lavoro, al computer, ogni volta che si deve allontanare, anche solo per poco tempo, dal proprio ufficio.
- ✓ Spetta all'incaricato mettere in atto gli accorgimenti ritenuti più opportuni affinché anche in sua assenza, il computer non resti incustodito e/o accessibile a terzi non autorizzati.
- ✓ In ogni caso deve essere attivata la funzione screen saver qualora l'incaricato si allontani, anche solo per pochi minuti, dal proprio ufficio.
- ✓ Risulta, inoltre, importante curare la conservazione e la segretezza della parola chiave evitando di trascriverla su supporto cartaceo precario o visibile (es. post-it) oppure di tenerla nel portafoglio o trascritta nella prima pagina dell'agenda o della rubrica di ufficio o in qualunque altro posto facilmente intuibile;

.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Inoltre l'utilizzo non corretto del servizio ReCUP – scuola potrebbe comportare l'immediata sospensione dell'accesso allo servizio stesso nonché la disattivazione dell'utenza senza preavviso;

Obblighi inerenti ai trattamenti senza l'ausilio di strumenti informatici

Le istruzioni di seguito riportate sono vincolanti per l'operatore scolastico solo se correlate all'attività lavorativa assegnata.

Per le operazioni di trattamento dei dati personali effettuate senza l'ausilio di strumenti elettronici, l'incaricato del trattamento deve osservare le misure di sicurezza adottate dalla struttura scolastica di appartenenza
Nel dettaglio si elencano di seguito le regole principali che l'incaricato deve osservare nelle operazioni di trattamento dei dati personali.

- I documenti che contengono dati personali non devono essere portati al di fuori dei locali individuati per la loro conservazione, se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Nel periodo di tempo in cui i documenti che contengono dati personali si trovano al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non deve lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti che contengono dati personali, composti da numerose pagine o più raccoglitori, siano sempre completi ed integri.
- Al termine dell'orario di lavoro, l'incaricato del trattamento deve riportare tutti i documenti che contengono dati personali nei locali (Archivi) individuati per la loro conservazione.
- I documenti (Faldoni, Raccoglitori, Fascicoli, etc.) che contengono dati personali non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Risulta necessario adottare ogni cautela affinché persone non autorizzate non vengano a conoscenza dei dati personali contenuti nei documenti utilizzati per lo svolgimento delle attività lavorative.
- Per evitare il rischio di divulgazione dei dati personali si deve limitare l'utilizzo di copie fotostatiche. Particolare cautela deve essere adottata quando i documenti sono consegnati in originale ad un altro incaricato debitamente autorizzato.

Risulta inoltre vietato:

- Effettuare copie fotostatiche o di qualsiasi altra natura - non autorizzate dal proprio Responsabile - di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati personali oggetto del trattamento.
- Sottrarre, cancellare, distruggere - senza l'autorizzazione del proprio Responsabile - stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati personali oggetto del trattamento.
- Consegnare - a persone non autorizzate dal proprio Responsabile - stampe, tabulati, elenchi, rubriche e, più in generale, ogni altro materiale che contiene dati/informazioni personali oggetto del trattamento.

In riferimento, invece, agli obblighi inerenti alla sicurezza degli archivi cartacei nonché alla sicurezza nella cancellazione dei dati si elencano le seguenti regole che l'incaricato deve osservare.

<u>Sicurezza Archivi Cartacei</u>

- L’accesso agli Archivi cartacei è limitata al solo personale autorizzato al trattamento e ai soli dati la cui conoscenza sia strettamente necessaria per adempiere alle attività lavorative assegnate.

La chiave degli archivi è fornita ai soli soggetti autorizzati.

Nel caso di dati sensibili, inoltre, devono essere osservate le seguenti regole:

- Le cartelle o fascicoli o supporti cartacei di vario genere che contengono dati personali devono essere conservati in armadi (Archivi) muniti di serratura con chiave che devono essere chiusi al termine della giornata di lavoro dall’incaricato del trattamento.
- Maggiori cautele devono essere utilizzate per i documenti e/o atti che contengono dati sensibili; in particolare i menzionati dati affidati all’incaricato del trattamento, qualora non vengano utilizzati, devono essere conservati in contenitori chiusi a chiave (es. cassettiere) fino al loro rientro in archivio.

Ai fini della sicurezza degli Archivi cartacei, sono stati adottati dispositivi di sicurezza passiva come rilevatori di fumo, allarme, estintori.

<u>Sicurezza nella cancellazione dei dati</u>

- La cancellazione dei dati personali può essere effettuata – previa autorizzazione del proprio Responsabile di Ufficio - quando la conservazione degli stessi non è più necessaria per legge e/o per gli scopi per cui sono stati raccolti e successivamente trattati.
- I dati personali possono essere cancellati anche su richiesta dell’interessato al trattamento (anche ai fini dell’esercizio del diritto all’oblio) - sempre che la conservazione non sia necessaria per legge e/o per la gestione del rapporto di lavoro (e/o contrattuale nel caso di consulenti e/o fornitori) - e comunque previa autorizzazione del proprio Responsabile di Ufficio.
- L’eventuale distruzione dei dati deve essere effettuata con sistemi meccanici o automatizzati in modo da evitare ogni possibile recupero. In caso di cancellazione dei dati memorizzati sui files elettronici, l’incaricato è tenuto al rispetto dei regolamenti/procedure adottate (es. utilizzo funzione “svuotamento del cestino in modalità sicura”) nonché delle istruzioni impartite dal proprio Responsabile.
- I documenti che contengono dati personali forniti alla struttura scolastica per la gestione del rapporto di lavoro e/o per l’esecuzione della propria attività lavorativa e/o per l’esecuzione di contratti con fornitori/consulenti esterni (ivi comprese l’esecuzione delle attività formative del personale dipendente) dovranno essere restituiti e/o cancellati – previa autorizzazione del Responsabile - alla cessazione del rapporto di lavoro e/o estinzione del rapporto contrattuale e/o comunque in tutti i casi in cui il trattamento dei dati personali non risulta essere più necessario per il perseguimento delle finalità suindicate, salvo diversa prescrizione di legge.

In ogni caso l’incaricato del trattamento ha l’obbligo di controllare e custodire i dati personali oggetto del trattamento in modo da evitare o, comunque, ridurre al minimo i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

L'accesso agli archivi contenenti dati sensibili deve essere controllato dal Responsabile di Ufficio. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, devono essere identificate e registrate su istruzione del Responsabile. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

* * *

Per quanto non previsto nel presente atto, si precisa che sarà cura del Responsabile dell'ufficio di appartenenza dell'incaricato nominato con il presente atto fornire ogni altra istruzione e/o raccomandazione in ordine alle operazioni di trattamento dei dati personali, alla gestione e custodia degli stessi nel rispetto della vigente normativa in materia di Privacy.

La presente nomina si intende valida per tutta la durata delle attività lavorative assegnate inerenti la gestione delle prenotazioni di esami COVID 19 – campagna Recup scuola. In caso di cessazione del rapporto di lavoro (anche interruzione temporanea delle attività lavorative come ad es. nei casi di aspettativa, congedi parentali, maternità, etc.) e/o cambiamento delle mansioni affidate, è vietato comunicare e/o divulgare dati personali di cui l'incaricato è venuto a conoscenza nell'espletamento delle mansioni lavorative assegnate.

Anzio 17/8/2020

IL DIRIGENTE SCOLASTICO
PROF.SSA MARIA ROSARIA VILLANI

Firmato da:
Il Dirigente Scolastico
Prof.ssa Maria Rosaria Villani
22/08/2020 15:17:02