I. C. S. - "G. DI VITTORIO"-PALERMO
Prot. 0010593 del 21/09/2026
III (Uscita)

DISPOSIZIONE DI SERVIZIO DEL DIRIGENTE SCOLASTICO

ATTO DI AUTORIZZAZIONE

– Misure finalizzate alla corretta attuazione alle disposizioni del Regolamento (UE) 679/2016 e del D.Lgs. 196/2003 così come modificato e novellato dal D.Lgs. 101/2018 –

OGGETTO: Nomina delle Persone Autorizzate al trattamento dei dati personali, ai sensi degli artt. 4 e 29 del Regolamento Europeo 679/2016 e integrazione delle istruzioni al personale dipendente.

IL DIRIGENTE SCOLASTICO

Visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito solo GDPR);

Visto il D.Lgs. 30 Giugno 2003, n.196 "Codice in materia di protezione dei dati personali";

Visto il D.Lgs. del 10 Agosto 2018 n.101 "Adeguamento al Regolamento UE 2016/679";

Visto il D.P.R. 13 giugno 2023, n. 81, Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165».;

Visto il D.Lgs. 7 marzo 2005, n. 82 "Codice dell'Amministrazione Digitale" e ss.mm.ii.;

Rilevato che, ai fini dell'osservanza delle disposizioni contenute nel GDPR, vanno innanzitutto individuati gli attori, i ruoli e le responsabilità del sistema organizzativo preordinato a garantire la protezione dei dati personali;

Richiamati gli articoli 4 e 29 del Regolamento Europeo 679/2016, che in particolare dispongono:

<u>Art. 4 (definizioni)</u>

"[…] ... «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;

<u>Art. 29 (Trattamento sotto l'autorità del Titolare del trattamento […])</u>

"[…] ... chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento … […]

Constatato che:

- è necessario attuare la migliore qualità conseguibile nel trattamento dei dati personali e ciò è possibile attuando in piena autonomia la gestione dei compiti all'interno della scuola;

- Risulta necessario configurare l'articolazione scolastica, secondo criteri di efficienza e efficacia, delegando compiti operativi a personale che possieda abilità e formazione opportune per svolgere le mansioni a esso delegate;

DISPONE

1) Di individuare il personale con il ruolo di "**ASSISTENTE AMMINISTRATIVO**" quali Persone autorizzate al trattamento (ex artt. 4 e 29 del Regolamento Europeo 679/2016)" per i trattamenti necessari per l'espletamento delle mansioni ricoperte all'interno della Scuola.
2) Di autorizzare il suddetto personale alle operazioni di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, comunicazione (nei soli casi autorizzati dal titolare), selezione, estrazione di dati, connesse alle funzioni e attività esercitate nelle seguenti aree di competenza (in base all'assegnazione disposta dal Dirigente scolastico):
   - Area didattica (alunni e genitori): gestione archivi elettronici e cartacei, consultazione documenti e registri di attestazione dei voti e di documentazione della vita scolastica dello studente, nonché delle relazioni tra scuola e famiglia, gestione contributi e tasse scolastiche, adempimenti connessi al registro infortuni e alle gite scolastiche-
   - Area personale (ATA e docenti): gestione archivi elettronici e cartacei, tenuta documenti e registri relativi alla vita lavorativa dei dipendenti-
   - Contabilità e finanza: gestione archivi elettronici della contabilità, gestione stipendi e pagamenti, nonché adempimenti di carattere previdenziale, gestione documentazione ore di servizio, gestione acquisti e rapporti coi fornitori, gestione Programma annuale e fondo di Istituto, registri contabili previsti dalla normativa vigente.
   - Protocollo, archivio e corrispondenza ordinaria.
   - Attività organi collegiali: per operazioni di consultazione ed estrazione dei dati dai verbali degli organi collegiali.
3) Per lo svolgimento delle suddette operazioni avrà accesso a postazioni informatiche e caselle di posta elettronica (personali e/o condivise), nonché ad applicazioni software per la gestione della segreteria digitale.
4) Di dare atto che ogni dipendente che cessa di far parte o perde il ruolo di "Assistente Amministrativo" cessa automaticamente dalla funzione di persona autorizzata al trattamento.
5) Ogni nuovo dipendente che entra a far parte o assume il ruolo di "Assistente Amministrativo" assume automaticamente la funzione di persona autorizzata al trattamento e che, pertanto, l'elenco delle persone autorizzate appartenenti a questa categoria corrisponde all'elenco dei dipendenti validamente in servizio che ne fanno parte.
6) Di autorizzare questa categoria di persone autorizzate al trattamento a trattare tutti i dati personali comuni e le categorie particolari di dati personali di cui all'art.9 del Regolamento Ue 2016/679 e dei dati personali relativi a condanne penali e reati di cui all'art.10 del Regolamento Ue 2016/679, con cui entrino in contatto nell'ambito dell'espletamento dell'attività di loro competenza o contenuti nelle banche dati, in archivi cartacei e informatici anche frammentari, dell'intera scuola;
7) Di autorizzare il personale con il ruolo di "Assistente Amministrativo" a trattare i dati suddetti

nel rispetto di tutte le misure di sicurezza previste dalla legge ed in particolare dal Regolamento UE 2016/679.

8) Di mettere a disposizione tutto il materiale informativo e legislativo necessario per approfondire la conoscenza della materia, nonché di organizzare appositi corsi di formazione in materia di privacy.

9) Di consegnare, all'atto dell'assunzione in servizio, a ogni nuovo componente (anche temporaneo) con il ruolo di "Assistente Amministrativo" copia del presente atto di nomina.

10) Di puntualizzare che i compiti e le funzioni a tal fine assegnate sono analiticamente elencate in calce al presente provvedimento, con facoltà di successiva integrazione e/o modificazione, dando atto che l'attribuzione di compiti e funzioni inerenti al trattamento dei dati personali non implica l'attribuzione di compiti e funzioni ulteriori rispetto a quelli propri della qualifica rivestita ma conferisce soltanto il potere/dovere di svolgere i compiti le funzioni attribuite.

11) Di dare atto, altresì, che:

- tale ruolo ha validità per l'intera durata del rapporto / incarico di dipendenza;
- tale ruolo viene a cessare al modificarsi del rapporto / incarico di dipendenza;
- tale ruolo viene a cessare in caso di revoca espressa;
- tale ruolo non consente l'attribuzione ad altri soggetti di poteri e compiti qui previsti;
- al cessare di tale ruolo, rimane inibito e comunque non autorizzato ogni ulteriore esercizio dei compiti e delle funzioni trattamento dei dati personali oggetto del presente provvedimento, salvo che ciò sia imposto o consentito da una norma di Legge o da un provvedimento dell'autorità ovvero sia necessario ad esercitare o difendere un diritto.

NOTIFICA E COMUNICAZIONE DEL PRESENTE ATTO

La presente dovrà essere comunicata ai destinatari sopra "Autorizzati" a mezzo mail e sottoscritta digitalmente da tutti i destinatari mediante l'utilizzo Firma Elettronica Avanzata FEA.

IL DIRIGENTE SCOLASTICO

ANGELA MARCIANTE
21.09.2026 17:23:54
CEST

Documento informatico sottoscritto con firma digitale (*ex art. 24 D.Lgs. n.82 del 07/03/2005*)

ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI

ISTRUZIONI GENERALI

Nello svolgere le proprie funzioni, che comportino un trattamento di dati personali, il personale scolastico deve attenersi alle seguenti istruzioni:

1. le persone autorizzate al trattamento devono operare sotto la diretta autorità del Titolare del trattamento e devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni ricevute;
2. qualunque trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali dell'Istituto;
3. è vietata qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia strettamente funzionale allo svolgimento dei compiti affidati e comunque autorizzata dal titolare del trattamento, o da una norma di legge o di regolamento;
4. gli assistenti amministrativi autorizzati al trattamento hanno l'obbligo di mantenere il riserbo sulle informazioni di cui siano venuti a conoscenza nell'esercizio della loro funzione; tale obbligo permane anche dopo la cessazione dell'incarico, senza limiti temporali;
5. devono essere rispettate ed applicate tutte le misure di sicurezza previste dalla legge ed in particolare dal Regolamento UE 2016/679;
6. i dati personali devono essere trattati in modo lecito e corretto secondo le prescrizioni di cui al Reg. UE 679/16, nel rispetto dei principi generali di liceità, correttezza, trasparenza, esattezza, minimizzazione e di quanto riportato nel Registro delle Attività di Trattamento adottato dall'Istituto scolastico;
7. i dati personali oggetto dei trattamenti devono essere esatti ed aggiornati inoltre devono essere pertinenti, completi e non eccedenti le finalità per le quali vengono raccolti e trattati;
8. le persone autorizzate al trattamento sono tenute a partecipare agli interventi formativi organizzati dalla Istituto scolastico sui profili della disciplina sulla protezione dei dati personali in rapporto alle attività connesse alle loro mansioni;
9. le persone autorizzate al trattamento devono attenersi alle seguenti modalità operative: richiedere e utilizzare soltanto i dati necessari alla normale attività lavorativa; custodire i dati oggetto di trattamento in luoghi sicuri e non accessibili ai soggetti non autorizzati; non lasciare incustoditi i documenti e gli altri supporti, anche informatici, contenenti dati personali senza aver provveduto alla loro messa in sicurezza; provvedere alla tempestiva riconsegna della documentazione consultata per causa di lavoro a chi è incaricato della sua conservazione permanente; accertarsi che gli interessati abbiano ricevuto l'informativa prevista dal Regolamento; accertarsi dell'identità di terzi e della loro autorizzazione al ritiro della documentazione in uscita;

10. conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
11. le persone autorizzate al trattamento possono procedere alla comunicazione o alla diffusione dei dati solo nei casi previsti dal Regolamento, previa consultazione del DS o del DSGA;
12. le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) dovranno avvenire in forma riservata; se effettuate per scritto dovranno essere consegnate busta chiusa;
13. in caso di comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti per finalità istituzionali, queste (comunicazioni) vanno poste in essere seguendo le indicazioni fornite dall'Istituto scolastico e avendo presente la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti (es. è vietato l'invio di documenti o file contenente categorie particolari di dati mediante posta elettronica semplice o utilizzare strumenti quali "drop box" o "google drive" se non previamente autorizzati);
14. il trattamento delle categorie particolari di dati personali di cui all'art. 9 del Regolamento Ue 2016/679 e dei dati personali relativi a condanne penali e reati di cui all'art. 10 del Regolamento Ue 2016/679 è consentito nei limiti e secondo le modalità di cui agli artt. 9 e 10 del Regolamento, solo per lo svolgimento dei compiti istituzionali o per l'adempimento a obblighi di legge o di regolamento; i supporti e la documentazione contenenti tale tipologia di dati devono essere utilizzati con particolare accortezza e nel pieno rispetto delle misure di sicurezza apprestate dal Titolare;
15. le convocazioni dei Gruppi di lavoro operativo per l'inclusione (GLO) e i Piani educativi individualizzati (PEI) devono avvenire nel rispetto della riservatezza e della protezione dei dati personali degli interessati.

Le stesse istruzioni e prescrizioni cogenti sono obbligatorie anche per il trattamento di dati personali realizzato, interamente o parzialmente, con strumenti elettronici, contenuti in archivi/banche dati o destinati a figurarvi.

Qualunque violazione delle istruzioni operative indicate nel presente documento dà luogo a precise responsabilità, anche disciplinari, ai sensi delle norme contenute nel Regolamento UE 679/2016 e dell'art. 4 dello Statuto dei Lavoratori.

In particolare, per tali trattamenti la persona fisica Autorizzata al trattamento ha l'obbligo di utilizzo e gestione attenendosi alle seguenti istruzioni:

A) STRUMENTI ELETTRONICI IN GENERALE

1. i personal computer fissi e portatili ed i programmi per elaboratore su di essi installati sono uno strumento di lavoro e contengono dati riservati e informazioni personali di terzi ai sensi della normativa sulla protezione dei dati personali: vanno, pertanto, utilizzati e conservati, insieme ai relativi documenti esplicativi, con diligenza e cura, attenendosi alle prescrizioni fornite dal Titolare e nel rispetto delle indicazioni da questo fornite;

2. in generale tutti i dispositivi elettronici sono forniti per lo svolgimento della sua attività lavorativa, nell'ambito delle mansioni a questo affidate. L'uso per fini personali è da considerare pertanto eccezionale e limitato a comunicazioni occasionali e di breve durata, ad esclusione dei dispositivi per i quali è esplicitamente regolamentato l'uso per fini personali;
3. le impostazioni dei personal computer e dei relativi programmi per elaboratore installati sono predisposte dagli addetti informatici incaricati sulla base di criteri e profili decisi dal Titolare, in funzione della qualifica del dipendente, delle mansioni cui questo è adibito, nonché delle decisioni e della politica di utilizzo di tali strumenti stabilita dalla Scuola. Il dipendente non può modificarle autonomamente; può ottenere cambiamenti nelle impostazioni solo previa autorizzazione.
4. assicurarsi, in caso di sostituzione del computer utilizzato, che siano effettuate le necessarie operazioni di formattazione o distruzione dei supporti di memorizzazione dei dati;
5. rivolgersi tempestivamente, per difficoltà o questione inerente alla sicurezza, al Dirigente scolastico o al DPO;
6. per finalità di assistenza, manutenzione ed aggiornamento e previo consenso esplicito del dipendente stesso, l'Amministratore di Sistema o soggetti appositamente incaricati allo svolgimento di tale attività potranno accedere da remoto al personal computer del dipendente attraverso un apposito programma "software";
7. il dipendente è tenuto ad osservare le medesime precauzioni e cautele, ove queste siano applicabili e pertinenti rispetto allo specifico strumento utilizzato, in relazione a tutti i dispositivi elettronici di cui fa uso, tra cui ad esempio fax, fotocopiatrici, scanner, masterizzatori, telefoni fissi, cellulari, pen-drive e supporti di memoria.
8. al dipendente è consentito l'utilizzo degli strumenti informatici forniti dalla Scuola per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.
9. Eventuali alterazioni di registri e/o dati personali riguardanti gli alunni devono essere comunicati per iscritto al DS o DSGA.

La Scuola ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati.

B) PREDISPOSIZIONE DI ATTI E DOCUMENTI DA PUBBLICARE SUL SITO WEB ISTITUZIONALE

Il personale scolastico preposto alla pubblicazione di atti e documenti sul sito istituzionale della Scuola deve:

1. adottare opportuni accorgimenti prima di procedere alla pubblicazione sul sito internet istituzionale tra cui:
   - individuare se esiste un presupposto di legge o di regolamento che legittima la diffusione del documento o del dato personale;

- verificare, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni;
- verificare che siano sottratti all'indicizzazione (cioè alla reperibilità sulla rete da parte dei motori di ricerca) eventuali categorie particolari di dati (i c.d. dati sensibili) e i giudiziari.

Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee al loro rapporto di lavoro con l'amministrazione e in difformità alle disposizioni di cui al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità.

C) SITO WEB E UTILIZZO DI PIATTAFORME DIGITALI

1. utilizzare le piattaforme digitali autorizzate dall'Istituto scolastico tenendo presente i principi generali e le indicazioni disponibili nel Regolamento d'Istituto per l'utilizzo piattaforma multimediale autorizzata;
2. il sito web deve essere costantemente aggiornato; deve essere verificata regolarmente la presenza sul sito dei documenti, nel rispetto della normativa in materia di obblighi di pubblicità, trasparenza e diffusione di dati, informazioni e documenti da parte delle Pubbliche Amministrazioni; particolare cura dovrà essere riservata alle sezioni "Amministrazione Trasparente" e "Albo on line";
3. in caso di pubblicazioni sul sito web della scuola, assicurarsi che i documenti siano depurati da ogni informazione e dato personale non strettamente necessario (criterio di pertinenza e non eccedenza) lasciando solo i dati strettamente necessari alla finalità. Non pubblicare nel sito web dati personali particolari;
4. utilizzare le piattaforme digitali tenendo presente i principi generali e le indicazioni disponibili nel Regolamento d'Istituto per l'utilizzo della piattaforma multimediale autorizzata;
5. l'eventuale condivisione di documenti contenenti dati personali sullo spazio in Cloud istituzionale deve essere riservata agli autorizzati, limitata ai dati essenziali e pertinenti, collegati alla finalità istituzionale che si intende perseguire.

D) CREDENZIALI DI AUTENTICAZIONE INFORMATICA
(Password, username e accesso ai sistemi informatici)

1. per le banche dati informatiche e gli applicativi in cloud, utilizzare sempre il proprio codice di accesso personale (es. SPID o CIE), evitando di operare su terminali altrui ed astenendosi dall'accedere a servizi telematici non consentiti;
2. le credenziali di autenticazione informatica sono individuali e devono essere custodite con cura e diligenza; non possono essere messe a disposizione né rivelate a terzi; non possono essere lasciate incustodite, né in libera visione.

   In caso di smarrimento e/o furto, bisogna darne immediata notizia al responsabile (o, in caso di assenza del responsabile, al titolare) del trattamento dei dati;
3. è vietato comunicare a terzi gli esiti delle proprie interrogazioni delle banche dati;

4. i codici identificativi, le *password* e le *smart card* saranno disattivate nel caso in cui i dipendenti cessino il loro rapporto di lavoro, oltre che nei casi espressamente e tassativamente previsti dalla normativa. In tali casi il dipendente è tenuto a restituirle agli uffici a ciò preposti.
5. la *password* che la persona fisica designata e autorizzata al trattamento imposta, con il supposto e l'assistenza, in caso di difficoltà, dell'Amministratore di Sistema (se esistente):
6. deve essere sufficientemente lunga e complessa e deve contemplare l'utilizzo di caratteri maiuscoli e speciali e numeri (almeno 10 caratteri);
   - non deve essere riconducibile alla persona;
   - deve essere cambiata almeno ogni 3/6 mesi;
   - non deve essere rivelata o fatta digitare al personale di assistenza tecnica;
   - non deve essere rivelata o comunicata al telefono, via fax od altra modalità elettronica;
   - non memorizzare *password* su dispositivi dell'Istituto o apparecchiature personali;
7. se si utilizza un PC condiviso, avere cura di accedere con il proprio *account* e disconnetterlo al termine dell'utilizzo;
8. eseguire sempre il corretto *logout* dagli account personali al termine della sessione di lezione, per evitare accessi non autorizzati e garantire la riservatezza dei dati trattati (es. registro elettronico e/o *account* personale piattaforme multimediali);
9. trattare i dati personali mediante l'utilizzo di apparecchiature in possesso dell'Istituzione scolastica;
10. non memorizzare dati personali su dispositivi dell'Istituto o apparecchiature personali;
11. in caso di perplessità in merito alla scelta delle soluzioni comportamentali più corrette da adottare, le persone autorizzate devono consultarsi con il Titolare o con il Responsabile onde evitare di incorrere in violazioni di legge;
12. informare tempestivamente il Titolare o il responsabile del trattamento di ogni circostanza idonea a determinare pericolo di dispersione o utilizzazione non autorizzata;

E) ASSENZA OD IMPOSSIBILITÀ TEMPORANEA O PROTRATTA NEL TEMPO

1. nell'ipotesi di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività del Titolare sia necessario accedere ad informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, il dipendente può delegare a un altro dipendente a sua scelta ("fiduciario") il compito di verificare il contenuto di messaggi e inoltrare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività deve essere redatto apposito verbale e informato il dipendente interessato alla prima occasione utile;
2. in caso di assenza o impossibilità, temporanea o protratta nel tempo, del dipendente, qualora per ragioni di sicurezza o comunque per garantire l'ordinaria operatività dell'ufficio sia necessario

accedere a informazioni o documenti di lavoro presenti sul personal computer del dipendente, inclusi i messaggi di posta elettronica in entrata ed in uscita, ed il dipendente non abbia delegato un suo fiduciario, secondo quanto sopra specificato, il Dirigente scolastico può richiedere con apposita e motivata richiesta all'Amministratore del Sistema di accedere alla postazione e/o alla casella di posta elettronica del dipendente assente, in modo che si possa prendere visione delle informazioni e dei documenti necessari. Contestualmente, il Dirigente scolastico deve informare il dipendente dell'avvenuto accesso appena possibile, fornendo adeguata spiegazione e redigendo apposito verbale;

3. in caso di allontanamento anche temporaneo dal posto di lavoro, o comunque dal luogo dove vengono trattati i dati, la persona autorizzata dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti non incaricati, di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento;
4. in caso di allontanamento anche temporaneo dalla postazione di lavoro (personal computer fisso o portatile), il dipendente non deve lasciare il sistema operativo aperto con la propria *password* e/o *smart card* inserita. Al fine di evitare che persone estranee effettuino accessi non consentiti, il dipendente deve attivare il salvaschermo con password o deve bloccare il computer e togliere la *smart card* dall'apposito alloggiamento.

F) UTILIZZO DELLA RETE INTERNET E RELATIVI SERVIZI - CLOUD STORAGE

1. non è consentito navigare in siti web non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare le opinioni politiche, religiose o sindacali del dipendente;
2. è da evitare la registrazione a servizi on-line, a titolo o per interesse personale;
3. non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati e con il rispetto delle normali procedure di acquisto;
4. non è permessa la partecipazione, per motivi non professionali, a servizi di forum, l'utilizzo di chat-line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);
5. il dipendente si impegna a circoscrivere gli ambiti di circolazione e di trattamento dei dati personali (es. memorizzazione, archiviazione e conservazione dei dati in cloud) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione Europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.).

G) POSTA ELETTRONICA

1. la casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa;
2. l'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa

riconducibili e non può in alcun modo compromettere la sicurezza o la reputazione della Scuola. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti al servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale;

3. si invitano i dipendenti a non utilizzare gli indirizzi di posta elettronica istituzionali assegnati per le comunicazioni personali;
4. al fine di garantire la continuità all'accesso dei messaggi da parte dei soggetti adibiti ad attività lavorative che richiedono la condivisione di una serie di documenti si consiglia e si incoraggia l'utilizzo abituale di caselle di posta elettronica condivise tra più lavoratori o delle caselle di posta istituzionali della Scuola, eventualmente affiancandoli a quelli individuali;
5. le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente.
6. non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o che possano essere in qualunque modo fonte di responsabilità della Scuola;
7. il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dalla Scuola. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile;
8. la posta elettronica diretta all'esterno della rete della Scuola può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti contenenti dati personali di cui agli articoli 9 e 10 del GDPR;
9. non è consentito l'utilizzo dell'indirizzo di posta elettronica istituzionale della Scuola per la partecipazione a dibattiti, Forum o mail-list, salvo diversa ed esplicita autorizzazione;
10. qualora si verifichino anomalie nell'invio e ricezione dei messaggi di posta elettronica sarà cura del dipendente informare prontamente l'Amministratore di sistema o il Dirigente scolastico.
11. nei casi di inoltro di e-mail a più destinatari è obbligatorio utilizzare la funzionalità di invio per copia conoscenza nascosta (*ccn*).

H) SOFTWARE, APPLICAZIONI E SERVIZI ESTERNI

1. onde evitare pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore, è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dall'Amministratore di sistema o figura analoga ovvero dal Dirigente scolastico.
2. non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
3. non è consentito modificare le configurazioni impostate sul proprio PC;

4. non è consentito configurare gli strumenti per la gestione della posta elettronica per la gestione di *account* privati. Non è inoltre consentito utilizzare detti strumenti per la ricezione, visualizzazione ed invio di messaggi a titolo personale;
5. il Titolare si riserva la facoltà di procedere alla rimozione di ogni file od applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti od installati in violazione delle presenti istruzioni;
6. tutti i software caricati sul sistema operativo ed in particolare i software necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi, (salvo quando questo sia richiesto dall'amministratore di sistema per compiere attività di manutenzione o aggiornamento).

I) RETI DI COMUNICAZIONE

1. nel caso di trattamento di dati personali effettuato mediante elaboratori non accessibili da altri elaboratori (cioè mediante computer stand alone) è necessario utilizzare la parola chiave (password) fornita per l'accesso al singolo PC;
2. nel caso di trattamento di dati personali effettuato mediante elaboratori accessibili da altri elaboratori, solo in rete locale, o mediante una rete di telecomunicazioni disponibili al pubblico, è necessario: utilizzare la parola chiave (password) fornita per l'accesso ai dati, oltre a servirsi del codice identificativo personale per l'utilizzazione dell'elaboratore;
3. le unità di rete o lo spazio all'interno del Registro elettronico sono aree di condivisione di informazioni strettamente professionali e non possono, in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque "file" che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità;
4. al fine di garantire la disponibilità dei documenti di lavoro assicurandone il backup periodico, si dovrà procedere al loro salvataggio nell'apposita area di rete individuale o di gruppo a ciò dedicata e disponibile sui sistemi server del Titolare;
5. non collegare dispositivi che consentano un accesso, non controllabile, ad apparati della rete del Titolare.
6. non condividere file, cartelle, hard-disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine condividere materiale elettronico tutelato dalle normative sul diritto d'autore (software, file audio, film, etc.).

J) SUPPORTI ESTERNI DI MEMORIZZAZIONE

1. utilizzare i supporti di memorizzazione solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
2. nel caso in cui per l'esercizio delle attività sopra descritte sia inevitabile l'uso di supporti rimovibili (quali ad esempio chiavi USB, CD-ROM, ecc), su cui sono memorizzati dati personali, essi vanno

custoditi con cura e non devono essere messi a disposizione o lasciati al libero accesso di persone non autorizzate;

3. proteggere i dati personali archiviati su supporti esterni con le stesse misure di sicurezza previste per i supporti cartacei;
4. verificare che i contenitori degli archivi/banche dati (armadi, cassettiere, computer, etc.) vengano chiusi a chiave e/o protetti da password in tutti i casi di allontanamento dalla postazione di lavoro;
5. evitare che i dati estratti dagli archivi/banche dati possano divenire oggetto di trattamento illecito;
6. copie di dati personali su supporti amovibili sono permesse solo se parte del trattamento; copie di dati contemplati dagli articoli 9 e 10 del GDPR devono essere espressamente autorizzate. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
7. evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione.
8. procedere alla cancellazione dei supporti esterni contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;
9. verificare l'assenza di virus nei supporti utilizzati.

K) INTELLIGENZA ARTIFICIALE

1. è consentito l'utilizzo dei soli strumenti di Intelligenza Artificiale (IA) autorizzati dall'Amministrazione;
2. gli strumenti e i sistemi di IA devono essere utilizzati garantendo il rispetto della normativa in materia di protezione dei dati personali. Nello specifico, nel rispetto del principio di minimizzazione dei dati, devono essere forniti in fase di input solo i dati strettamente necessari per il raggiungimento delle finalità specifiche, evitando di inserire dati personali, compresi i dati particolari ex art. 9 del GDPR, o riservati, salvo espressa autorizzazione da parte dell'Istituto scolastico;
3. l'utilizzo degli strumenti di IA deve avvenire nel rispetto delle istruzioni impartite e delle misure di sicurezza implementate, evitando qualsiasi trattamento non autorizzato di dati personali, al fine di prevenire danni, attacchi informatici e manipolazione dei dati;
4. qualora i sistemi e gli strumenti di IA siano impiegati per attività che comportano processi decisionali automatizzati, deve essere garantito il controllo umano, consentendo così di mantenere la supervisione e l'autonomia umana nel processo decisionale e di assicurare la salvaguarda contro potenziali discriminazioni e/o bias, nonché la tutela dei diritti e le libertà fondamentali degli interessati;
5. l'utilizzo di strumenti e sistemi di IA è consentito esclusivamente per attività strettamente connesse allo svolgimento delle mansioni lavorative e solo con account istituzionali autorizzati e ambienti autorizzati e gestiti dall'Amministrazione;

6. si raccomanda un uso corretto, trasparente e responsabile degli strumenti di IA, garantendo sempre la verifica dei risultati e dei contenuti generati dai sistemi di IA;
7. si raccomanda di utilizzare gli strumenti di IA come *chatbot, Large Language Model (LLM)* solo per attività generiche e mai per contenuti sensibili o critici;
8. è necessario garantire l'integrità dei dati, in quanto l'immissione di dati dannosi in un sistema di IA può modificarne il comportamento.

L) ISTRUZIONI PER IL TRATTAMENTO DI DATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

1. Le pratiche e i fascicoli contenenti dati personali (di seguito: "le pratiche") devono essere di norma riposte in archivi chiusi. Si considera archivio chiuso anche il locale chiuso a chiave;
2. le pratiche e i fascicoli devono essere prelevati, a cura degli utilizzatori, solo nella misura e per il tempo strettamente necessari per lo svolgimento dei relativi compiti, al termine dei quali – ed in ogni caso al termine della giornata lavorativa – devono essere riposte negli archivi. Ciascun utilizzatore deve aver cura di verificare che le pratiche affidategli non restino incustodite, specie in contesti accessibili a soggetti non incaricati del trattamento (aree di passaggio, sale d'attesa, sale riunioni, ecc.);
3. anche durante la giornata lavorativa, in caso di allontanamento dalla postazione di lavoro per un periodo di tempo significativo, le pratiche devono essere riposte negli archivi, salvo adeguata garanzia di controllo da parte di altri utilizzatori autorizzati ai medesimi trattamenti. In ogni caso le pratiche non devono essere mai lasciate incustodite;
4. lo smarrimento o il furto di informazioni devono essere comunicati immediatamente ai referenti della procedura sui Data Breach;
5. è buona regola evitare la proliferazione eccessiva di stampe e fotocopie di documenti contenenti dati personali. Le stampe e le fotocopie inutili devono essere distrutte nell'apposito distruggi-documenti, se disponibile, oppure devono essere strappate in pezzi piccoli;
6. oltre a quanto previsto per i dati personali in genere, le pratiche e i fascicoli contenenti categorie particolari di dati e dati relativi a condanne penali o reati devono essere conservati in archivi ad accesso controllato, devono essere controllate e custodite fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione (ivi compresi altri utilizzatori che non siano autorizzati ad accedere alle informazioni sensibili), e devono essere restituite al termine delle operazioni affidate;
7. quando circolano all'interno dell'Istituto scolastico devono essere inserite in busta chiusa; stesso discorso qualora vi fosse la necessità di comunicare tali dati e documenti ad altri Enti (es. Comuni o ASL) autorizzati in forza di norma di legge o regolamento a riceverli;
8. compete agli utilizzatori il controllo della chiusura a chiave degli armadi contenenti tale tipologia di dati e la chiusura dei propri uffici in caso di temporaneo allontanamento ed alla fine dell'orario lavorativo. I documenti contenenti dati ultra-sensibili (es. stato di salute relativo ad alunni con BES

o DSA) devono essere custoditi in cassaforte o in archivio separato.

Scarti di archivio

1. Gli scarti di archivio, ossia il periodico smaltimento di materiale cartaceo contenente dati personali, deve essere effettuato evitando che le informazioni personali, specie se sensibili, possano essere trattate da soggetti non incaricati/autorizzati.
2. In particolare i documenti contenenti categorie particolari si dati devono essere smaltiti mediante utilizzo degli appositi strumenti per la distruzione, ove disponibili, altrimenti vanno ridotti in piccoli pezzi.

Consegna di certificazioni medico-sanitarie a mezzo di altri soggetti

1. La consegna di certificazioni mediche, o comunque di altre informazioni personali delicate relative ai dipendenti, alluni o terzi può essere effettuata anche tramite altri dipendenti o comunque altre persone a condizione che:
   - la documentazione sia di regola consegnata in busta chiusa;
   - prima della consegna, la documentazione non sia lasciata incustodita. Di regola, ove non sia presente il destinatario, la documentazione va consegnata a un responsabile o superiore gerarchico;
   - la consegna avvenga nel minor tempo possibile.

M) ISTRUZIONI DA SEGUIRE IN CASO DI DATA BREACH

Nel caso in cui vi sia il fondato sospetto che si sia verificata una violazione di dati, come ad esempio:

- Perdita di documenti o fascicoli
- Distruzione archivi
- Furto o smarrimento di strumenti elettronici contenenti dati personali
- Sospetto di accesso non autorizzato nei locali deputati all'archiviazione
- Sospetto di accesso non autorizzato nella sala Server
- Sospetto di accesso non autorizzato nel proprio PC
- Comportamento anomalo del proprio PC o dispositivo informatico
- Etc.…

Occorre informare tempestivamente i referenti della procedura sui Data Breach, comunicandogli il maggior numero di dettagli circa la violazione subita:

- Data in cui è avvenuto l'evento o in cui si è venuti a conoscenza.
- Modalità di esposizione al rischio, ad es.: Lettura dei dati personali, Copia dei dati personali, Alterazioni dei dati personali, Cancellazione dei dati personali, Furto dei dati personali.
- Dati personali oggetto della violazione (dati dei dipendenti, degli alunni etc.).