ISTITUTO COMPRENSIVO STATALE DI ODERZO (TV)
SCUOLE INFANZIA - SCUOLE PRIMARIE - SCUOLA SECONDARIA 1° GRADO
Piazzale Europa 21 – 31046 ODERZO (TV)- ☏ 0422/815655 🖷 0422/814578
E-mail TVIC88400X@Istruzione.it – Posta Certificata: TVIC88400X@pec.istruzione.it
C.F. 94141320260 - Cod. Min.:TVIC88400X – SITO: www.icoderzo.edu.it

N. Circolare e data vedi segnatura

A tutto il personale
I.C. ODERZO

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:

Art. 4 (definizioni)

"[…] ... «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;

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

"[…] ... 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 i dipendenti nel ruolo di "Docenti", "personale ATA", "assistenti tecnici", 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 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;
3) **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.
4) **DI DARE ATTO** che il presente provvedimento integra l'atto/gli atti a suo tempo adottato/i

NOTIFICA E COMUNICAZIONE DEL PRESENTE ATTO

La presente dovrà essere comunicata ai destinatari sopra "Autorizzati" a mezzo PEO/PEC/Registro Elettronico o altre modalità individuate dalla Scuola

Oderzo, 09/10/2023

IL DIRIGENTE SCOLASTICO
Dott.ssa Francesca MENEGHEL

Firmato digitalmente da **Francesca MENEGHEL**
C=IT
O=Istituto Comprensivo Statale di Oderzo **94141320260**

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

SOTTO IL PROFILO DEL TRATTAMENTO DI DATI PERSONALI:

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

- in attuazione del principio di «liceità, correttezza e trasparenza»,
  - le operazioni di raccolta, registrazione, elaborazione di dati ed in generale, le operazioni di trattamento tutte, avvengono agli esclusivi fini dell'inserimento o arricchimento degli archivi/banche dati della Scuola, nell'osservanza delle tecniche e metodologie in atto;
  - autorizzazione a comunicare o eventualmente diffondere o trasferire all'esterno i dati personali esclusivamente ai soggetti autorizzati a riceverli legittimamente, per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute dal Titolare del trattamento;
- in attuazione del principio di «minimizzazione dei dati», obbligo di trattamento dei soli ed esclusivi dati personali che si rivelino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui è preposto;
- in attuazione del principio di «limitazione della finalità» il trattamento deve essere conforme alle finalità istituzionali del Titolare e limitato esclusivamente a dette finalità;
- in attuazione del principio di «esattezza», obbligo di assicurare l'esattezza, la disponibilità, l'integrità, nonché il tempestivo aggiornamento dei dati personali, ed obbligo di verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali i dati sono stati raccolti, e successivamente trattati;
- in attuazione del principio di «limitazione della conservazione»
  - 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 e obbligo di esercitare la dovuta diligenza affinché non vengano conservati, nella Scuola, dati personali non necessari o divenuti ormai superflui. Alla conclusione del trattamento, obbligo di assicurarsi che i documenti contenenti i dati di cui agli articoli 9 e 10 del GDPR vengano conservati in contenitori/armadi muniti di serratura od in ambienti ad accesso selezionato e vigilato, fatte salve le norme in materia di archiviazione amministrativa;
- in attuazione del principio di «integrità e riservatezza» obbligo di garantire un'adeguata sicurezza dei dati personali, compresa la protezione, dando diligente ed integrale attuazione alle misure logistiche, tecniche informatiche, organizzative, procedurali definite dal Titolare, trattando i dati stessi con la massima riservatezza ai fini di impedire trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. In particolare:
  - riporre in archivio, al termine del periodo di trattamento, i supporti ed i documenti, ancorché non definitivi, contenenti i dati personali;
  - non fornire dati personali per telefono, qualora non si abbia certezza assoluta sull'identità del destinatario;
  - evitare di inviare, per e-mail, documenti in chiaro contenenti dati personali: si suggerisce, in tal caso, di inviare la documentazione, senza alcun esplicito riferimento all'Interessato (ad esempio, contrassegnando i documenti semplicemente con un codice);
- in attuazione del principio di «trasparenza»:

- accertarsi dell'identità dell'Interessato, prima di fornire informazioni circa i dati personali od il trattamento effettuato;
- fornire all'Interessato (o verificare che siano state fornite) tutte le informazioni di cui agli articoli 13 e 14 del GDPR e le comunicazioni di cui agli articoli da 15 a 22 ed all'articolo 34 del GDPR, relative al trattamento utilizzando apposita modulistica. Se richiesto dall'Interessato, le informazioni medesime possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'Interessato;
- agevolare l'esercizio dei diritti dell'Interessato ai sensi degli articoli da 15 a 22 del GDPR;

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.

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

- ✓ 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;
- ✓ 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;
- ✓ 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.
- ✓ assicurarsi, in caso di sostituzione del computer utilizzato, che siano effettuate le necessarie operazioni di formattazione o distruzione dei supporti di memorizzazione dei dati;
- ✓ rivolgersi tempestivamente, per difficoltà o questione inerente alla sicurezza, al Dirigente scolastico o al DPO;
- ✓ 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";
- ✓ 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.
- ✓ 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.

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:

- ✓ 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) **Password e username (credenziali di autenticazione informatica)**

- ✓ per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui ed astenendosi dall'accedere a servizi telematici non consentiti. Le credenziali di autenticazione informatica sono individuali. Non possono essere condivise;
- ✓ è vietato comunicare a terzi gli esiti delle proprie interrogazioni delle banche dati;
- ✓ i codici identificativi, le password e le smart card saranno disattivati 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.
- ✓ 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):
  - deve essere sufficientemente lunga e complessa e deve contemplare l'utilizzo di caratteri maiuscoli e speciali e numeri (almeno 8 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;

D) Assenza od impossibilità temporanea o protratta nel tempo

- ✓ 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.
- ✓ 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.

E) Log-out

- ✓ 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**

- ✓ 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;
- ✓ è da evitare la registrazione a servizi on-line, a titolo o per interesse personale;
- ✓ 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;
- ✓ 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);
- ✓ 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

- ✓ la casella di posta elettronica è uno strumento finalizzato allo scambio di informazioni nell'ambito dell'attività lavorativa;
- ✓ 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 il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale;
- ✓ si invitano i dipendenti a non utilizzare gli indirizzi di posta elettronica istituzionali assegnati per le comunicazioni personali;
- ✓ 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;
- ✓ le comunicazioni via posta elettronica devono avere un contenuto espresso in maniera professionale e corretta nel rispetto della normativa vigente.
- ✓ 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;

- ✓ 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;

- ✓ 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;

- ✓ 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;

- ✓ 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.

H) **Software, applicazioni e servizi esterni**

- ✓ 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.

- ✓ non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

- ✓ non è consentito modificare le configurazioni impostate sul proprio PC;

- ✓ 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;

- ✓ 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;

- ✓ 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**

- ✓ 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;

- ✓ 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;

- ✓ 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;

- ✓ 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;
- ✓ non collegare dispositivi che consentano un accesso, non controllabile, ad apparati della rete del Titolare.
- ✓ 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) Utilizzo dei mezzi di informazione e dei social media

- ✓ nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla Scuola di appartenenza;
- ✓ in ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine della Scuola;
- ✓ al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media. Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.

K) Supporti esterni di memorizzazione

La persona fisica designata e autorizzata al trattamento, ha l'obbligo di:

- 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;
- proteggere i dati personali archiviati su supporti esterni con le stesse misure di sicurezza previste per i supporti cartacei;
- 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;
- evitare che i dati estratti dagli archivi/banche dati possano divenire oggetto di trattamento illecito;
- 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;
- evitare di asportare supporti informatici o cartacei contenenti dati personali di terzi, senza la previa autorizzazione.
- procedere alla cancellazione dei supporti esterni contenenti dati personali, prima che i medesimi siano riutilizzati. Se ciò non è possibile, essi devono esser distrutti;
- verificare l'assenza di virus nei supporti utilizzati.