ISTRUZIONI OPERATIVE SUL CORRETTO TRATTAMENTO DEI DATI PERSONALI

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione dovrà essere eseguita nel rispetto delle seguenti istruzioni operative al fine di evitare la dispersione e/o perdita dei dati trattati:

- custodire i documenti cartacei e i supporti informatici removibili in scaffali, cassetti e armadi possibilmente chiusi a chiave e, al termine dell'orario di lavoro, riporre tutti i documenti presenti sulla scrivania in cassetti chiusi a chiave, soprattutto quando la pulizia degli uffici è affidata a ditte esterne.
- Accertarsi, anche durante i trattamenti, che i documenti contenenti dati personali non siano alla portata di vista di persone non autorizzate.
- Verificare, in caso di allontanamento anche temporaneo dalla postazione di lavoro, o comunque dal luogo dove vengono trattati i dati, che non vi sia possibilità da parte di terzi, anche dipendenti non incaricati, di accedere a dati personali per i quali è in corso un qualunque tipo di trattamento.
- Consentire l'accesso agli archivi contenenti dati particolari o giudiziari solo alle persone autorizzate, creando accessi logici e di autenticazione ad applicativi o a cartelle condivise secondo ruoli e responsabilità definiti e profili personali attribuiti agli utenti al fine di migliorare la sicurezza e la gestione dei dati archiviati. Si suggerisce inoltre di separare i dati particolari e/o giudiziari, contenuti in supporti informatici e in faldoni, da quelli non particolari e/o giudiziari in partizioni differenti nonché applicare controlli di sicurezza diversi ai dati particolari, ad esempio attraverso anonimizzazione o pseudonimizzazione.
- Garantire la sicurezza dei dati attraverso la distruzione di documenti o fotocopie non necessari o non più utilizzati. La cancellazione deve avvenire in maniera irreversibile, assicurando l'indisponibilità dei documenti archiviati tramite, ad esempio, l'utilizzo di dispositivi distruggi documenti o l'eliminazione definitiva dai supporti informatici, ad esempio svuotando il cestino del PC e formattando i supporti di memoria esterni.

- Accertarsi della distruzione di documenti inutilizzati contenenti dati personali, particolari e giudiziari.

- Evitare la comunicazione e la diffusione di documenti contenenti dati personali al di fuori dalla sede scolastica, in originale o in copia, se non dietro espressa autorizzazione del Titolare del trattamento.

- Effettuare le comunicazioni agli interessati (persone fisiche a cui afferiscono i dati personali) **SEMPRE** in forma riservata; in particolare nel caso di comunicazioni a mezzo lettera, dovranno essere consegnate in buste chiuse. Se trasmesse tramite posta elettronica, occorre adottare **adeguati protocolli di sicurezza** quali la trasmissione cifrata del file, ad esempio con formato compresso tipo .zip, rar, ecc. protetto da password (password da inviarsi separatamente e con sistema diverso da quello utilizzato per inviare il file); all'atto della consegna di documenti contenenti dati personali l'incaricato dovrà assicurarsi dell'identità dell'interessato o di chi è stato delegato al ritiro del documento in forma scritta; è opportuno che tutti i documenti contenenti dati relativi lo stato di salute e altri dati particolari siano consegnati direttamente agli uffici amministrativi competenti al fine di evitarne la dispersione o perdita durante la trasmissione.

- Utilizzare sempre i canali istituzionali per le comunicazioni elettroniche ad alunni, colleghi, genitori, personale della scuola o altri soggetti coinvolti, avendo sempre presente il principio di minimizzazione e di riservatezza delle comunicazioni stesse e dei dati coinvolti.

- Garantire la riservatezza ed integrità dei messaggi di posta elettronica; è vietato cedere a terzi qualsiasi informazione, anche in forma sintetica, sul contenuto del messaggio ricevuto tramite posta elettronica. L'Utente si assume ogni responsabilità penale e civile ed il carico di ogni eventuale onere derivante dall'uso improprio del servizio.

- all'atto della consegna/inoltro/invio di documenti contenenti dati personali l'incaricato dovrà altresì verificare la corrispondenza tra il documento da trasmettere e il soggetto destinatario della comunicazione.

- tutte le comunicazioni elettroniche rivolte a più destinatari dovranno essere eseguite in **copia conoscenza nascosta (CCN)** per evitare di rendere pubblici dati personali a tutti i destinatari.

- **Epurare dai documenti**, per i quali vi è un obbligo di pubblicazione in capo all'Amministrazione, **tutti i dati personali non strettamente necessari** al raggiungimento delle finalità di pubblicità e trasparenza dell'istituto.
- Tutte le attrezzature informatiche (PC, LIM, schermi TV ecc) della Scuola devono essere utilizzate esclusivamente per lo svolgimento delle attività didattiche, per le esigenze dell'ufficio di segreteria e di Presidenza e in generale per tutte le attività didattiche o propedeutiche alla gestione degli alunni e genitori, personale ATA e Docenti, contabilità e finanza, protocollo e archivio, corrispondenza ordinaria.
- **non è consentito servirsi delle attrezzature informatiche per uso personale** e/o privato.
- le apparecchiature tecnologiche (hardware, software e configurazioni varie) sono gestite dall'amministratore di sistema e/o dalle ditte incaricate della manutenzione.
- è fondamentale **custodire con cura e diligenza le credenziali** per l'accesso ai servizi informatici, aggiornandole con frequenza (possibilmente ogni tre mesi), non divulgandole né cedendole a terzi per alcun motivo ed evitando di salvarle nel pc, utilizzando sistemi di memorizzazione automatica.
- **assicurarsi di aver eseguito il logout** da qualsiasi piattaforma web o dai programmi utilizzati e spegnere correttamente tutte le attrezzature utilizzate (PC, Lim, notebook, tablet, proiettori, ecc.) al termine della sessione di lavoro, non solo per evitare accessi non autorizzati ma anche per garantire il corretto funzionamento delle stesse.
- **non salvare documenti contenenti dati personali sulla memoria del computer** o su altri dispositivi elettronici (videocamera, fotocamera ecc..) dotati di scheda di memoria (tutte le attrezzature vengono ciclicamente formattate, pertanto i dati presenti vengono cancellati senza preavviso); se necessario, utilizzare servizi di cloud storage (Google Drive, Dropbox, Icloud, One Drive, ecc.) istituzionali o dispositivi di memoria rimovibili, ricorrendo sempre a sistemi di archiviazione sicuri (pseudonimizzare o cifrare i documenti). Al termine del lavoro, rimuovere e cancellare dalla memoria del computer o di altri dispositivi elettronici (videocamera, fotocamera ecc..) i dati personali eventualmente presenti.
- Non scaricare o salvare file di origine incerta sul PC, né aprire o inoltrare e-mail provenienti da mittenti sconosciuti o appartenenti a catene e mail lists.
- Il salvataggio di dati, documenti e cartelle deve avvenire su server o in cloud. È opportuno seguire il principio di clear screen ("schermo pulito"), evitando di

conservare i file sul desktop del PC per assicurare la disponibilità degli stessi in caso di malfunzionamento o compromissione della macchina.

- Riporre tutte le attrezzature mobili in armadietti chiusi a chiave al termine dell'attività di laboratorio.
- Non lasciare incustoditi i laboratori durante le attività e accertarsi che siano chiusi al termine delle stesse.
- Informare tutti gli utenti dei laboratori delle regole di utilizzo delle attrezzature approvate dall'Istituto.
- Il personale deve, prima di lanciare una stampa, verificare che le impostazioni di stampa e la carta presente nel cassetto della stampante siano adeguate alle sue esigenze.
- Qualora, a stampa iniziata, il personale dovesse riscontrare anomalie, ad esempio perché la stessa non risponde alle sue aspettative, il medesimo deve annullare prontamente il prosieguo premendo il tasto annulla sulla stampante stessa.
- Una volta inviato in stampa il file il personale deve prontamente recarsi presso la stampante e raccogliere il documento.
- Nel caso in cui la stampante non dovesse funzionare correttamente, è necessario eliminare la coda di stampa, operazione che può svolgere da solo dal PC che ha utilizzato.
- È vietato lasciare nel cassetto di uscita della stampante il documento inviato.
- Il personale è tenuto a segnalare prontamente eventuali guasti delle attrezzature contattando il personale tecnico di competenza.
- Ogni responsabilità relativa al corretto uso delle macchine è attribuito al personale scolastico utilizzatore.

Il Dirigente Scolastico

Giorgio Lucibello