ISTRUZIONI OPERATIVE PER IL TRATTAMENTO DEI DATI

(Ai sensi del Reg. UE 2016/679 e del D. Lgs 101/2018)

1. Glossario

Vengono di seguito riportate le definizioni dei concetti che ricorrono più spesso all'interno del presente documento. Per un'analisi più approfondita si rimanda al testo del Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, e al D. Lgs 101/2018, recante le disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE 2016/679.

Custode delle password: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati;
Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
Destinatario: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi;
Incaricato del Trattamento: la persona fisica, nominata dal titolare o dal responsabile del trattamento, autorizzata al trattamento dei dati personali, secondo quanto indicato nella lettera di incarico, che agisce sotto l'autorità diretta del titolare o del responsabile;
Interessato: il soggetto (persona fisica) al quale si riferiscono i dati personali;
Responsabile Del Trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
Responsabile Della Protezione Dati: la persona fisica, nominata dal titolare o dal responsabile del trattamento, che collabora con il titolare e con il responsabile del trattamento per il rispetto delle disposizioni del Regolamento 2016/679 del Parlamento Europeo.
Titolare Del Trattamento: la persona fisica o 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
Il titolare del trattamento è l'Ente (ISTITUTO SCOLASTICO) e la titolarità è esercitata dal rappresentante legale (DIRIGENTE SCOLASTICO);
Trattamento: 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;

2. Premessa

Al fine di permettere una corretta e sicura gestione dei dati trattati all'interno dell'Istituto Scolastico, gli Incaricati del trattamento (di seguito "Incaricato") provvedono a rispettare le seguenti istruzioni operative, con il supporto del Titolare del trattamento (di seguito "Titolare"), del Responsabile del trattamento (di seguito "Responsabile") e del Responsabile di protezione dei dati (di seguito "RPD").
Nell'ambito dello svolgimento delle proprie mansioni, è necessario e doveroso innanzitutto fare riferimento agli obblighi riportati nell'atto di nomina con cui l'Incaricato viene autorizzato al trattamento dei dati per conto del Titolare.

L'Incaricato deve impegnarsi a:

- trattare dati personali soltanto su istruzione documentata del Titolare e/o del Responsabile del trattamento;
- adottare tutte le misure di sicurezza previste nell'Art. 5 del Regolamento Europeo;
- assistere il Titolare e/o il Responsabile del trattamento con misure tecniche e organizzative adeguate a proteggere i dati personali e atte a garantire il rispetto degli obblighi previsti dal Regolamento Europeo (Artt. Da 32 a 36);
- cancellare o restituire tutti i dati personali al Titolare e/o al Responsabile del trattamento al termine della validità del presente Atto di Nomina;
- mettere a disposizione del Titolare e/o al Responsabile del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal Regolamento Europeo;
- collaborare alle attività di revisione, vigilanza e controllo realizzate dal Titolare e/o al Responsabile del trattamento;
- informare immediatamente il Titolare e/o al Responsabile del trattamento qualora, a suo parere, un'istruzione violi delle disposizioni in materia di privacy.

3. Istruzioni operative

Di seguito sono riportate le istruzioni operative divise nella seguente modalità:

1. Istruzioni generali;
2. Utilizzo degli strumenti elettronici;
3. Gestione autenticazione informatica (nome utente e password);
4. Gestione dei dati in formato cartaceo;

3.1 Istruzioni generali

- Il trattamento dei dati personali deve avvenire da parte degli incaricati seguendo quanto riportato nel Piano di Lavoro in corso di validità ed in riferimento alle disposizioni stabilite dal Titolare e/o Responsabile;
- I dati personali trattati devono essere:
  - pertinenti alla mansione da svolgere;
  - non eccedenti le necessità del lavoro;
  - corretti e tempestivamente aggiornati;
  - trattati in modo da ridurre al minimo i rischi:
    - di distruzione o perdita;
    - di accesso agli stessi da parte di persone non autorizzate;
    - di trattamento non autorizzato.
- Gli incaricati devono:
  - nel limite del possibile, tenere chiuso a chiave il proprio ufficio, con chiave in possesso dei soli autorizzati;
  - a fronte della richiesta di conoscenza di dati personali provenienti da parte di persone diverse dall'interessato, verificare la legittimità della richiesta stessa ed eventualmente rifiutarsi di fornire i dati a chi non ne abbia il diritto.
- In generale occorre:
  - non lasciare incustoditi pratiche contenenti informazioni su persone fisiche o giuridiche;
  - non lasciare incustoditi i terminali ed i dispositivi recanti i registri elettronici di classe, in special modo se accessibili o visibili dall'esterno;
- L'accesso ai locali contenenti dati personali è permesso solo alle persone autorizzate, secondo quanto riportato nel Manuale di Gestione Privacy e quanto stabilito dal Titolare e dal Responsabile;
- È vietato commentare con colleghi e/o soggetti esterni all'Istituto Scolastico i dati sensibili e/o giudiziari di cui si dovesse venire a conoscenza nello svolgimento del proprio lavoro;
- L'obbligo di mantenere la dovuta riservatezza in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, deve permanere in ogni caso, anche quando sia venuto meno l'incarico stesso.

3.2 Utilizzo degli strumenti elettronici

- L'uso delle apparecchiature informatiche che contengono dati personali è permesso solo per svolgere le attività previste nelle istruzioni impartite agli incaricati;
- L'elaboratore assegnato per lo svolgimento dei compiti d'ufficio deve essere adoperato e custodito con attenzione. Monitor e tastiera costituiscono una finestra aperta su archivi e dati: un comportamento superficiale espone al rischio di conseguenze anche penali. Pertanto si richiede di:
  - impostare l'attivazione di uno screen-saver (funzione salva schermo) con richiesta di password per ristabilire la sessione di lavoro in corso se la postazione viene lasciata incustodita durante l'orario di lavoro;
  - assicurarsi di aver spento i propri elaboratori al termine della giornata di lavoro;
  - non abbandonare la propria postazione incustodita per periodi lunghi;
  - nell'abbandonare la postazione chiudere i documenti cui si sta lavorando;
  - non lasciare la postazione collegata in rete se non c'è necessità;
  - chiudere la propria sessione di lavoro o disconnettersi ogni volta che ci si assenta;
  - evitare di prendere documenti da computer esterni, e comunque sempre verificare file e dischi provenienti da terzi.
- Garantire il mantenimento delle funzioni ottimali dei sistemi elettronici contattando il responsabile della manutenzione degli strumenti elettronici:
  - prima di effettuare qualsiasi operazione incerta del risultato;
  - appena si notano disfunzioni a livello hardware, software o nei sistemi di protezione (antivirus e firewall);
  - prima di installare dispositivi hardware od applicazioni;
  - se sono stati accidentalmente scaricati virus o dialer (programmi che modificano il numero di telefono chiamato) da internet o dalla posta elettronica.
- Gli incaricati autorizzati ad accedere ad internet devono utilizzare solo i servizi cui sono abilitati;
- Gli incaricati non sono autorizzati a scaricare alcun tipo di software sia esso freeware o shareware senza il consenso del Titolare e/o Responsabile;
- Gli incaricati devono conservare i dati sensibili in formato elettronico contenuti sui PC in maniera criptata, con password di accesso in possesso dei soli autorizzati al trattamento;
- In merito alla gestione della posta elettronica, gli incaricati:
  - non devono aprire messaggi provenienti da indirizzi sconosciuti e/o con oggetto differente dall'attività che viene svolta, né gli eventuali allegati;
  - non devono inviare per posta elettronica informazioni riservate o particolarmente delicate per l'interessato senza adottare misure di protezione specifiche;
  - devono filtrare i messaggi di entrata al fine di escludere la presenza di virus;
- Nel caso in cui per l'esercizio delle attività 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, né messi a disposizione o lasciati al libero accesso di persone non autorizzate;
- I supporti rimovibili contenenti dati personali se non utilizzati vanno distrutti o ripuliti dai dati contenuti;
- In caso di comunicazioni elettroniche per finalità istituzionali, queste comunicazioni vanno poste in essere seguendo le indicazioni fornite dall'Istituzione Scolastica e avendo presente la necessaria riservatezza delle comunicazioni stesse e dei dati coinvolti.

3.3 Gestione autenticazione informatica (nome utente e password)

La password è un elemento fondamentale della sicurezza delle informazioni.
La password identifica in modo univoco l'utente del computer e dei servizi informatici. Inoltre permette l'accesso ad aree riservate di software, portali e siti internet utilizzati quotidianamente per lo svolgimento delle attività formative ed amministrative. Non è conveniente usare una sola password per accedere a diversi servizi, poiché può compromettere la sicurezza degli account. E' bene quindi creare una password differente per ogni servizio usato.
La tendenza a condividere le password aumenta il rischio di perderne il possesso ed essere acquisite per scopi malevoli. È dunque essenziale che la password sia mantenuta riservata e non comunicata ad altri.
Per un'accorta creazione e una corretta conservazione delle password è necessario rispettare le seguenti indicazioni:

- una password sicura deve essere lunga almeno 8 caratteri alfanumerici, contenere caratteri speciali (per esempio +#$_^) e possedere sia minuscole che maiuscole;
- la password non dovrebbe contenere parole comuni come per esempio "password" piuttosto che "qwerty" o "1234";
- la password non deve essere banale o facilmente individuabile;
- la password non deve coincidere con nomi propri o nomi comuni o date;
- la password non deve contenere il nome utente o il proprio nome o altre informazioni personali quali il codice fiscale;
- la password deve essere mantenuta riservata e non comunicata ad altri utenti. Se eccezionalmente dovesse essere necessario fornirla in caso di emergenza ad altra persona, va cambiata subito dopo;
- la password non possono essere lasciate incustodite, né in libera visione, ma deve essere annotata su supporti cartacei od elettronici, a patto che non sia facilmente reperibile da altri (es. password scritta su foglio conservato in cassetto chiuso a chiave);
- non è consentito usare l'opzione, che alcuni software come Internet Explorer offrono, di salvare automaticamente la password per successivi utilizzi delle applicazioni;
- il periodo massimo di validità della password è di 6 mesi; dopo tale periodo è necessario sostituire la password con una nuova diversa dalla precedente;
- non deve essere ripetuta una password usata in passato;
- Non è consentito che due persone accedano al sistema con lo stesso identificativo utente;
- Gli incaricati devono assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e sicurezza del sistema. A tal fine, è necessario prevedere un sistema che agevoli il reperimento delle password anche in assenza dell'incaricato. Tale procedura è descritta nel Manuale di Gestione Privacy, all'interno del quale viene individuato anche il soggetto responsabile del suo corretto svolgimento, il Custode della password, addetto a conservare le password utilizzate dagli incaricati in un luogo chiuso e protetto;
- In caso di smarrimento e/o furto della password gli incaricati devono darne immediata notizia al Responsabile e/o al Titolare

3.4 Gestione dei dati in formato cartaceo

Gli archivi contenenti dati personali devono essere custoditi in modo da ridurre al minimo i rischi di perdita degli stessi e di accesso da parte di persone non autorizzate. Gli incaricati, in riferimento ai supporti cartacei contenenti dati personali, devono pertanto rispettare le seguenti indicazioni:

- Mantenere i documenti cartacei ordinati e aggiornati;
- Riporre i documenti, quando non sono necessari, negli appositi contenitori quali archivi, cassetti e armadi muniti di serratura ed in luoghi non direttamente accessibili a persone non autorizzate, avendo cura che le chiavi di apertura dei contenitori siano conservate in un luogo sicuro e segreto, noto solo al personale autorizzato;
- Dismettere, secondo le disposizioni del responsabile, i dati personali che non sono più necessari per le finalità dell'attività;
- È vietato effettuare copie fotostatiche o di qualsiasi altra natura di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento per scopi diversi da quelli autorizzati dal responsabile;
- È vietato sottrarre, cancellare, distruggere, senza l'autorizzazione del responsabile, stampe, tabulati, elenchi, rubriche ed ogni altro materiale riguardante i dati oggetto del trattamento;
- È vietato consegnare a persone non autorizzate stampe, tabulati, elenchi, rubriche ed ogni altro materiale riguardante i dati oggetto del trattamento.