



Al Prof. Bruno MANNINI

Oggetto: Istruzioni per il trattamento di dati personali nell'ambito di gestione e supervisione del sistema informatico e della rete della Scuola e contestuale designazione quale Amministratore di Sistema

L'Istituto Istruzione Superiore "Piero Martinetti", in persona del Dirigente Scolastico *pro tempore* (di seguito, la "Scuola"), in qualità di Titolare del trattamento dei dati personali raccolti nell'ambito della propria organizzazione,

premessi che:

- a) ha rilasciato al Prof. Bruno Mannini, nella sua qualità di docente, apposita autorizzazione al trattamento dei dati personali di cui lo stesso viene a conoscenza nell'ambito dello svolgimento della propria attività professionale;
- b) la predetta autorizzazione contiene precise istruzioni per la sicurezza e il corretto svolgimento delle operazioni di trattamento dei dati personali;
- c) viste le Sue specifiche competenze e conoscenze informatiche e dei sistemi e strumenti in uso presso la Scuola, è altresì addetto alla gestione e supervisione del sistema informatico (hardware e software), della rete e degli apparati di sicurezza informatica della Scuola (di seguito, a) e b) complessivamente l'"Incarico");
- d) nell'ambito dell'Incarico, può dunque conoscere, anche indirettamente o accidentalmente, dati personali;

e considerato che:

- e) ai sensi dell'art. 29 del Regolamento (UE) 2016/679 "*chiunque agisca sotto... [l'] autorità ...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*",
- f) al contempo, il Provvedimento Generale del Garante per la protezione dei dati personali del 27/11/2008, come modificato dal successivo Provvedimento del 25/06/2009 (di seguito, complessivamente, il "Provvedimento"), ha previsto alcune prescrizioni specifiche per coloro che svolgono le funzioni di Amministratore di Sistema, intendendosi per tale colui che in ambito informatico svolge una delle seguenti attività: gestione di impianti di elaborazione o sue componenti; manutenzione di impianti di elaborazione o sue componenti; gestione di basi di dati; gestione di reti; gestione apparati di sicurezza; amministrazione di sistemi software complessi;

tutto ciò premesso e considerato,

La AUTORIZZA espressamente

a compiere - con strumenti sia cartacei, sia elettronici e con modalità automatiche e manuali - le operazioni di trattamento di dati personali limitatamente a quanto necessario all'attuazione dell'Incarico secondo le seguenti **informazioni e istruzioni** e di quelle che verranno di volta in volta comunicate dalla Scuola (come nell'ambito



di circolari, ordini di servizio, policy, regolamento per il corretto funzionamento delle funzioni strumentali, *etc.*) e comunque nel rispetto della normativa vigente in materia di protezione dei dati personali.

1. Ambito di trattamento

1.1. Potrà svolgere le operazioni di trattamento funzionali all'esecuzione dell'Incarico, quali, a titolo esemplificativo:

- a. raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, raffronto o interconnessione, limitazione, cancellazione o distruzione dei dati personali;
- b. ogni attività connessa con le operazioni sopra indicate, nel rispetto delle norme di legge applicabili, quali a titolo esemplificativo:
 - consultazione e aggiornamento *database* fornitori (con l'indicazione dei relativi referenti) degli strumenti tecnici o di componenti del sistema informatico o di servizi inerenti;
 - eventuale gestione di tutte le informazioni riguardanti reclami, segnalazioni, richieste dei docenti/collaboratori in merito alle attrezzature di laboratorio;
 - manutenzione ordinaria hardware e software del Titolare, anche mediante accesso con connessione remota;
 - manutenzione ordinaria server dati (compreso il ripristino dello stato dei servizi in caso di interruzione) e relativo backup;
 - primi interventi di miglioramento/manutenzione sul sistema e relativo backup/recovery;
 - gestione delle problematiche relative alla sicurezza e all'ottimizzazione del sistema e della rete;
 - adozione di provvedimenti necessari a evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico degli stessi con copie di back-up, vigilando sulle procedure attivate in struttura;
 - più in generale, gestione e supervisione di tutte le operazioni (anche accidentali) di trattamento dei dati personali necessarie all'esecuzione dell'Incarico.

1.2. Nei limiti di quanto necessario all'attuazione dell'Incarico e viste le operazioni di trattamento derivanti, potrà avere accesso e conoscere:

- i dati personali contenuti nel server della Scuola e comunque nei sistemi oggetto dell'Incarico;
- forniti direttamente dalla Scuola funzionalmente all'esecuzione e organizzazione dell'Incarico;
- rinvenibili in occasione dell'esecuzione dell'Incarico (come *account* o *indirizzo IP* degli autorizzati ad accedere ai sistemi o comunque di coloro che vi accedono, log, *etc.*);



In particolare, detti dati: a) potranno riguardare i seguenti soggetti: alunni, genitori/tutori, docenti e personale amministrativo, collaboratori esterni (madrelingua, addetti a laboratori specifici o *extra* curricolari, *etc.*), nonché ulteriori fornitori (società o professionisti) che offrono servizi alla Scuola; b) di norma appartengono alla categoria di dati comuni. È però possibile che, nello svolgimento delle attività di assistenza e manutenzione ai sistemi informatici della Scuola, Lei possa venire a conoscenza di dati *particolar conservati* in appositi file/cartelle, come ad esempio eventuali dati sanitari (disabilità, allergie, *etc.*) o esigenze (anche di tipo etnico o religioso) dello studente o del personale, appartenenza del personale dei sindacati, eventuali esigenze religiose del personale che possono incidere sull'organizzazione della Scuola (turni, ferie, *etc.*).

1.3. Si precisa che salvo espressa e diretta autorizzazione (anche verbale) della Scuola, non è autorizzato a eseguire trattamenti con finalità diverse da quelle strettamente necessarie per l'esecuzione delle funzioni connesse all'Incarico e comunque è tenuto ad eseguire le operazioni di trattamento affidateLe attenendosi esclusivamente alle istruzioni impartite dalla Scuola.

2. Modalità di esecuzione delle operazioni di trattamento nell'ambito dell'Incarico – Istruzioni

2.1. Nella Sua qualità di Autorizzato al Trattamento e Amministratore di Sistema, è tenuto a:

- operare in modo lecito e corretto; pertanto, dovrà:
 - trattare i Dati Personali esclusivamente al fine di adempiere alle obbligazioni nascenti dal proprio ruolo e funzione e, in ogni caso, per gli scopi per i quali i Dati Personali sono stati raccolti;
 - verificare la completezza e la pertinenza dei Dati Personali trattati, nonché la loro non eccedenza rispetto alle finalità della relativa raccolta e del successivo trattamento;
 - compiere le operazioni di trattamento strettamente necessarie affinché i dati personali siano trattati il meno possibile;
 - prestare particolare attenzione ai dati classificati come particolari (già dati sensibili);
- procedere alle operazioni di trattamento in condizioni che assicurino che i Dati Personali a Lei affidati e i documenti/altri supporti in cui sono contenuti non siano accessibili a soggetti non autorizzati, seppure dipendenti o collaboratori della Scuola. I Dati Personali devono quindi essere protetti da accessi non autorizzati, che possono avvenire di persona (si pensi a un soggetto non autorizzato che entra fisicamente in un ufficio e prova a conoscere o sottrarre dati) o tramite contatti telematici o telefonici che possono rivelarsi truffaldini (ad esempio una telefonata mediante la quale il chiamante tenta di raccogliere determinati dati o informazioni);
- ove possibile, verificare l'esattezza dei Dati Personali trattati e, se necessario, opportunamente aggiornarli e/o informare direttamente il Dirigente di ogni variazione intervenuta o inesattezza constatata;
- custodire con cura i supporti esterni (es chiavette USB, dischi esterni, tablet, smartphone, *etc.*), evitando di lasciarli in luoghi non protetti, e i propri account ai drive e simili sistemi di condivisione di documenti;



Via Montello, 29
10014 CALUSO (TO)
Tel 011 9832445

Email: info@iismartinetti.edu.it
PEC: iois03900t@pec.istruzione.it
WEB: IISMARTINETTI.EDU.IT

CF: 93010900012
Codice fatturazione UFLC34
Codice univoco IPA istsc_tois03900t

5. in caso di interruzione, anche temporanea, delle operazioni di trattamento, verificare che i Dati Personali non siano accessibili a terzi non autorizzati. In particolare, i documenti cartacei contenenti Dati Personali, quando non presidiati, dovranno essere, conservati e custoditi in armadi/cassettiere adeguatamente chiusi o in altri contenitori protetti e non accessibili a soggetti non autorizzati. Parimenti, al fine di proteggere la documentazione memorizzata su supporti informatici, non dovrà lasciare incustodito il dispositivo a Lei assegnato (o anche a sua disposizione, in caso di dispositivi condivisi) con sessioni applicative aperte o con login effettuato, ma dovrà assicurarsi di proteggere il dispositivo e il relativo contenuto tramite l'uso di password o altri tipi di blocchi/controlli come, ad esempio, screen saver;
6. al termine di ciascuna attività che comporta un trattamento di dati personali (come la consultazione di documenti, l'archiviazione, *etc.*) e, in particolare, delle proprie ore di servizio, riporre/chudere i documenti/file contenenti i Dati Personali negli appositi archivi cartacei ed elettronici. Al termine delle ore di servizio i computer (desktop e portatili) in uso presso la sede scolastica devo essere spenti, a meno che per particolari ragioni tecniche o di servizio debbano rimanere in funzione (in tal caso, il computer acceso deve risiedere in un ufficio o in un locale chiuso a chiave o protetto e con salvaschermo attivo e protetto da credenziali);
7. non creare archivi o banche dati nuove senza espressa autorizzazione da parte della Scuola, né effettuare *backup*, anche parziali, su sistemi e supporti, anche rimovibili, diversi da quelli messi a disposizione dalla Scuola e senza il preventivo consenso di quest'ultima;
8. prestare attenzione alla stampa di documenti su stampanti condivise o fotocopiatrici di rete, avendo cura di recuperare tempestivamente la stampa e di non lasciare i documenti incustoditi. La protezione dei dati si applica anche a documenti cartacei, cui va garantita custodia e controllo. Non riutilizzare per appunti il retro di fogli stampati o fotocopiati se contengono dati personali. Qualora sia fornito, è sempre necessario utilizzare il "distruggi-documenti" per rendere non leggibili i documenti contenenti dati personali o informazioni rilevanti. Nel caso si debbano smaltire grandi moli di documenti cartacei connessi all'attività di ricerca e didattica (esempio documenti correlati a prove d'esame di studenti) e contenenti dati personali è necessario contattare il Dirigente Scolastico per ottenere l'autorizzazione da parte della Soprintendenza Archivistica competente e quindi fruire, nel caso, del servizio di gestione dei rifiuti;
9. garantire la massima riservatezza durante lo svolgimento delle operazioni di trattamento e quindi applicare le misure di sicurezza previste dalla presente lettera o comunque impartite, anche verbalmente, dalla Scuola. In particolare, è tenuto a conservare le proprie credenziali, così come l'eventuale parola chiave, con cura e la massima segretezza e utilizzarle in modo esclusivo, senza comunicarle ad altri, ad eccezione del Dirigente in caso di particolare necessità o urgenza;
10. segnalare prontamente alla Scuola ogni tentativo di violazione, illecito, errore e/o anomalia riscontrati; parimenti, in caso di smarrimento e/o furto delle Sue credenziali o qualora abbia il sospetto che le stesse siano state violate o apprese da terzi, dovrà darne immediata notizia al Dirigente e/o al personale tecnico addetto;



- 11.** mantenere sempre un atteggiamento prudentiale e rispondere sempre in maniera negativa a richieste di dati, effettuate in qualunque modo, che non pervengano chiaramente da soggetti autorizzati, e la cui identità, in caso di dubbio, non sia stata accuratamente verificata. Le richieste di dati devono avvenire obbligatoriamente in forma scritta e, nel caso, autorizzate dal Dirigente Scolastico. È vietato, altresì, fornire o rendere disponibili informazioni tecniche, riferite alla rete e ai sistemi della Scuola, alle policies e alle credenziali usate, ai software e alle applicazioni utilizzate, a soggetti esterni alla Scuola. Tali informazioni sono solitamente domandate per cercare di violare i sistemi della Scuola. Pertanto, in caso in cui si trovi a consegnare documentazione in uscita, dovrà verificare l'identità dei riceventi e la loro autorizzazione al ritiro. Le comunicazioni effettuate per scritto dovranno essere consegnate in contenitori chiusi ai diretti interessati o ai soggetti autorizzati a riceverle. Parimenti, non deve fornire telefonicamente dati e informazioni, senza avere la certezza dell'identità dei richiedenti;
- 12.** partecipare ai corsi di formazione finalizzati a renderlo edotto dei rischi connessi alle operazioni di trattamento ed alla sua istruzione circa le modalità per prevenire eventuali danni o dispersioni dei Dati Personali;
- 13.** proteggere la propria macchina, durante le assenze (anche brevi) dalla postazione di lavoro, con screen saver dotati di password idonee;
- 14.** applicare le misure di sicurezza impartite dalla Scuola in qualsiasi tempo, per iscritto o verbalmente e in particolare con le procedure eventualmente predisposte dalla Scuola per l'uso del proprio materiale informativo ed eventualmente dei device personali, ove esplicitamente consentiti dalla Scuola;
- 15.** con particolare riferimento alla Sua attività di amministratore di sistema:
 - sovrintendere alle risorse del sistema operativo di base dati e consentirne l'utilizzazione;
 - verificare che siano adottati tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati;
 - vigilare durante gli interventi in loco sull'applicazione delle procedure ed istruzioni definite; in caso di necessità trasferire al fornitore le apparecchiature elettroniche, parti di esse o supporti contenenti i dati oggetto della manutenzione; se l'oggetto della manutenzione non sono i dati stessi o il loro recupero, e se tecnicamente possibile, i supporti di registrazione devono essere cancellati prima dell'asporto (verificando se è necessario effettuare un backup);
 - proteggere i sistemi utilizzando configurazioni minime restrittive nei servizi e negli utenti di sistema, attivando solo i servizi realmente necessari. A tale proposito, si precisa che: i) le credenziali amministrative di autenticazione sui sistemi e strumenti informatici a Lei univocamente assegnate come Amministratore di Sistema devono essere utilizzate esclusivamente in relazione alle sessioni ed ai processi inerenti alla gestione e manutenzione dei sistemi stessi; è vietato l'utilizzo di tali credenziali per attività che per il loro svolgimento non necessitano di un privilegio amministrativo ma possono essere svolte attraverso le credenziali di utente standard (es. consultazione della casella di posta elettronica assegnata, utilizzo degli strumenti di Office Automation, navigazione Internet,



etc.); ii) le utenze generiche di tipo tecnico predisposte esclusivamente per l'avvio di servizi pianificati non devono essere utilizzate per effettuare accessi interattivi ai sistemi informatici; tali accessi sono consentiti esclusivamente con autenticazione attraverso le credenziali assegnate in via univoca.

2.2. Fermo restando quanto sopra, la Scuola rinvia alle ulteriori policy inerenti, ad esempio, al *Regolamento per il corretto uso del patrimonio informativo scolastico*, nonché a eventuali procedure o manuali in relazione a specifiche situazioni/modalità di svolgimento delle attività o inerenti alla gestione di eventi particolari (tra cui, ad esempio, incidenti informatici, violazione dei dati, *etc.*), riservandosi la facoltà di fornire, in ogni momento, ulteriori e diverse indicazioni in merito a tali aspetti.

3. Obblighi di riservatezza

3.1. Non potrà comunicare o diffondere i Dati Personali senza la preventiva autorizzazione scritta della Scuola (o dal referente dalla stessa designato), salvi i casi previsti dalla legge o in forza di ordini dell'Autorità giudiziaria.

3.2. I suddetti obblighi dovranno essere osservati per l'intera durata del rapporto di lavoro instaurato ed anche dopo la relativa cessazione, salvo in relazione a quei dati personali che la Scuola (anche in ragione dei propri doveri di trasparenza) abbia reso pubblici o che comunque siano divenuti lecitamente tali (non si considerano lecitamente pubblici quelli resi noti in violazione delle disposizione della Scuola e della normativa vigente e rilevante in materia), fermo restando che a prescindere dalla eventuale pubblicazione dei dati personali da parte della Scuola qualora ricorrano le basi giuridiche, è tenuto a rispettare i principi, limiti e divieti e le condizioni di liceità di trattamento di dati personali previsti dalla normativa vigente (anche con riferimento alle limitazioni di trattamento dei dati resi manifestamente pubblici).

4. Misure di sicurezza

È tenuto ad applicare le misure di sicurezza impartite dalla Scuola in qualsiasi tempo, per iscritto o verbalmente e in particolare con le procedure eventualmente predisposte dalla stessa per l'uso della Piattaforma e più in generale del proprio patrimonio informativo.

5. Informazioni raccolte dalla Scuola in relazione al profilo di Amministratori di Sistema

5.1. In forza del Provvedimento (e considerata la particolare delicatezza del ruolo di amministratore di sistema), la Scuola provvederà a:

i) raccogliere i log di accesso, disconnessione e tentativi di accesso generati dall'account a Lei assegnato, con credenziali di autenticazioni univoche, quale Amministratori di Sistema (con la conseguente possibilità di indentificare ciascun amministratore);

ii) includere i Suoi dati identificativi e le Sue funzioni in un documento interno periodicamente aggiornato e reso disponibile, su richiesta, alle Autorità competenti;

iii) comunicare o comunque rendere disponibile/conoscibile agli altri lavoratori della Scuola la Sua identità e le Sue funzioni, qualora, nell'espletamento delle Sue mansioni, dovesse trattare dati personali di tali altri lavoratori;



iv) verificare, con periodicità programmata a cadenza almeno annuale, le attività da Lei svolte quale Amministratore di Sistema, allo scopo di verificare la loro rispondenza alle mansioni effettivamente attribuite e alle misure organizzative, tecniche e di sicurezza adottate rispetto all'attuazione dei trattamenti di dati personali e ciò anche utilizzando i log di accesso ai sistemi informatici raccolti e registrati.

5.2. I dati raccolti (e quindi, oltre ai Suoi dati identificativi – tra cui, ad esempio, indirizzo IP, username – i dati/le informazioni sugli accessi – log – che, in qualità di Amministratore di Sistema, effettua ai sistemi e dispositivi della Scuola e quindi in generale login, logout, failed login –) saranno conservati per le finalità di sicurezza individuate dal Provvedimento e per l'attuazione degli adempimenti derivanti e con particolare riferimento ai log per un periodo massimo di 12 mesi (e comunque non inferiore a 6, come previsto dal Provvedimento stesso), decorsi i quali saranno cancellati.

5.3. Si precisa che:

- l'accesso ai Suoi dati personali inerenti allo svolgimento dell'attività connesse alla Sua funzione di Amministratore di Sistema (e quindi in particolare ai registri di log) è consentito solo a soggetti appositamente individuati e autorizzati dalla Scuola e che sono tenuti a rispettare un impegno/obbligo di riservatezza;
- il trattamento dei suddetti dati discende automaticamente dalla Sua funzione di Amministratore di Sistema; pertanto, il suo eventuale rifiuto od opposizione al trattamento da parte della Scuola di tali dati comporta l'impossibilità da parte Sua di ricoprire la funzione di Amministratore e, conseguentemente, potrebbe rendere difficoltosa la corretta attuazione del Suo rapporto di Lavoro con la Scuola.

5.4. Il presente paragrafo è da intendersi quale *addendum* all'informativa privacy "generale" già a Sue mani in merito ai trattamenti dei Suoi dati personali compiuti dalla Scuola nell'ambito del rapporto di lavoro con Lei in essere, riguardando nello specifico il trattamento dei dati personali derivante dalla funzione di Amministratore di Sistema.

6. Cessazione dell'autorizzazione e della designazione quale Amministratore di Sistema - Disposizioni finali

6.1. Alla cessazione del rapporto di lavoro con la Scuola, per trasferimento ad altra istituzione o cessazione del rapporto di lavoro per qualsiasi altra causa, dovrà interrompere ogni operazione di trattamento dei dati personali inerenti all'incarico e all'organizzazione della Scuola e garantire a quest'ultima tutto il necessario supporto per proseguire il trattamento in autonomia, anche adoperandosi per favorire il passaggio di consegne. In ogni caso, resta fermo quanto previsto al par. 3 in merito all'obbligo di riservatezza anche successivamente al termine del rapporto con la Scuola. Con particolare riferimento alla funzione di amministratore di Sistema si evidenzia che la Scuola potrà: a) modificare il Suo profilo di autorizzazione da soggetto Autorizzato con funzioni di Amministratore di sistema (in relazione agli Ambiti e agli Ambienti assegnati) ad autorizzato "semplice"; b) revocare la presente designazione in qualsiasi momento qualora dovesse cessare l'incarico con la Scuola o dovessero venire meno le Sue funzioni speciali indicate alla lettera b) delle premesse.



ISTITUTO DI ISTRUZIONE SUPERIORE "Piero MARTINETTI"



Via Montello, 29
10014 CALUSO (TO)
Tel 011 9832445

Email: info@iismartinetti.edu.it
PEC: tois03900t@pec.istruzione.it
WEB: IISMARTINETTILEDU.IT

CF: 93010900012
Codice fatturazione UFLC34
Codice univoco IPA istsc_tois03900t

6.2. La presente lettera di autorizzazione e designazione è rilasciata ai sensi della normativa sulla protezione dei dati personali e non Le attribuisce alcun diritto o aspettativa a ricevere qualsiasi ulteriore compenso, essendo l'adempimento delle relative istruzioni parte integrante della prestazione contrattuale e, come tale, già remunerato.

6.3. La Scuola potrà in qualsiasi momento fornire istruzioni aggiuntive, anche verbalmente, o modificare quelle precedentemente impartite. Per qualsiasi ulteriore informazione concernente la presente lettera e le operazioni a Lei affidate potrà rivolgersi al dirigente scolastico o ad altro soggetto dallo stesso indicato.

Il Dirigente Scolastico
Katia MILANO
(Documento informatico firmato
digitalmente ai sensi del T.U. 445/2000,
del D. Lgs. 82/2006 e norme collegate)