INDICE DELLE RIVISIONI				
DATA	REVISIONE	MOTIVO EMISSIONE	REDAZIONE	VERIFICA APPROVAZIONE
13/09/2025	00	definitiva	RSGQ	✓

INDICE

1. Introduzione

I dati trattati da **ISTITUTO MICHELANGELO BUONARROTI S.r.l.** (nel prosieguo anche l'"Istituto") nello svolgimento della propria attività costituiscono una parte vitale del patrimonio aziendale che pertanto deve essere tutelato.

Il Regolamento UE n. 679/2016 (*"Regolamento Generale sulla protezione dei dati personali - GDPR"*) ha introdotto obblighi a carico delle imprese la cui inosservanza è sanzionata anche penalmente ed espone a responsabilità civili.

Il trattamento di dati personali è sottoposto a regole e prescrizioni che impongono alle imprese di mettere in atto misure tecniche e organizzative adeguate per garantire che tali trattamenti siano eseguiti in modo da prevenire e ridurre al minimo i "rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati".

In particolare l'utilizzo delle tecnologie informatiche e telematiche, dal punto di vista tecnico, rappresentano un fattore di rischio che può essere contenuto se sono seguite precise indicazioni volte a garantire la sicurezza delle procedure.

L'*Autorità Garante per la protezione dei dati personali* (Garante della Privacy) prescrive, inoltre, ai datori di lavoro di:
- specificare le modalità di utilizzo ritenute corrette degli strumenti informatici, di internet e della posta elettronica messi a disposizione al personale che opera in azienda;
- indicare le regole di controllo che possono legittimamente effettuare sui medesimi strumenti ed attraverso di essi.

Il presente regolamento viene pertanto predisposto nel rispetto della vigente disciplina in materia di protezione dei dati personali nonché delle linee guida emanate a livello nazionale dal Garante della Privacy. Esso sostituisce il precedente regolamento consegnato a tutti gli Incaricati ed integra le specifiche istruzioni già fornite ai medesimi.

2. Definizioni

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. Sono considerati dati personali: - nome e cognome - indirizzo di casa - indirizzo email - numero identificativo nazionale - numero di passaporto - indirizzo IP (quando collegato ad altri dati) - numero di targa del veicolo - numero di patente - volto, impronte digitali o calligrafia - numeri di carta di credito - identità digitale - data di nascita - luogo di nascita - informazioni genetiche - numero di telefono - account name o nickname.
DATO SENSIBILE	**dato personale** idoneo a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
DATO GIUDIZIARIO	**dato personale** idoneo a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o idoneo a rivelare la qualità di imputato o indagato in un procedimento penale.
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 ovvero l'interconnessione, la limitazione, la cancellazione o la distruzione.
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.

RESPONSABILE DEL TRATTAMENTO	**la persona fisica, la persona giuridica, l'autorità pubblica, il servizio o altro organismo** che tratta dati per conto del Titolare del trattamento.
INCARICATO DEL TRATTAMENTO	la **persona fisica** autorizzata al trattamento dei dati personali sotto l'autorità del Titolare o del Responsabile.
INTERESSATO DEL TRATTAMENTO	la **persona fisica** cui si riferiscono i dati personali oggetto di trattamento

3. Organizzazione e responsabilità

TITOLARE del trattamento

È l'Istituto (Società), in persona del suo legale rappresentante, che determina le finalità e le modalità del trattamento, decidendo in ordine:

- a come esercitare le operazioni di trattamento dei dati (raccolta e registrazione dei dati con mezzi elettronici o su supporto cartaceo);
- alla qualità e alla quantità dei dati (adeguatezza, pertinenza, non eccedenza - minimizzazione - dei dati rispetto alle finalità);
- all'ambito di comunicazione e diffusione dei dati (determinazione dei soggetti destinatari delle operazioni);
- alle misure di sicurezza da adottare, affinché i trattamenti svolti non causino danni ai soggetti cui si riferiscono i dati, oltre a dover garantire la loro corretta conservazione.

Al TITOLARE spetta, quando abbia nominato uno o più RESPONSABILI, un generale dovere di vigilanza (anche attraverso verifiche periodiche) sulla puntuale osservanza delle disposizioni e delle istruzioni che ha impartito.

RESPONSABILE del trattamento

È una figura che può essere designata facoltativamente dal TITOLARE e deve essere individuata tra i soggetti che presentino garanzie sufficienti per mettere in misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Ai fini della sicurezza, ha le seguenti responsabilità:

- tratta i dati soltanto su istruzione del titolare;
- garantisce che le persone autorizzate al trattamento si siano impegnate alla riservatezza
- adotta le misure di sicurezza adeguate;

INCARICATI del trattamento

Con specifico riferimento alla sicurezza, hanno le seguenti responsabilità:

- svolgere le attività previste dai trattamenti secondo criteri e modalità previsti;
- non modificare i trattamenti esistenti, non introdurne di nuovi senza l'esplicita autorizzazione del TITOLARE;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il TITOLARE in caso di incidente di sicurezza che coinvolga dati personali;
- attenersi alle istruzioni impartite per la sicurezza dei locali e dei sistemi informatici descritte di seguito.

4. Prescrizioni di sicurezza

L'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo dell'Istituto deve sempre ispirarsi al principio della **diligenza** e **correttezza**, comportamenti che il dipendente/collaboratore è sempre tenuto ad adottare nell'ambito del rapporto di lavoro.

Anche le informazioni accessibili tramite l'applicazione web "Scuolaonline" mediante dispositivi personali dei collaboratori/dipendenti devono sottostare alle prescrizioni descritte nel presente regolamento

Poiché anche nella ordinaria attività lavorativa alcuni comportamenti possono mettere a rischio la sicurezza e l'immagine dell'Istituto, di seguito vengono richiamate le regole comportamentali finalizzate non tanto a censurare condotte consapevolmente scorrette (già di per sé proibite), ma soprattutto per evitare azioni che inconsapevolmente possano causare rischi alla sicurezza del trattamento dei dati.

Sicurezza dei locali in cui si trattano i dati personali

Per le aree della direzione e della segreteria si individuano le seguenti prescrizioni:

- sono autorizzati ad accedervi gli INCARICATI al trattamento;
- i visitatori occasionali devono essere accompagnati.

Sicurezza dei supporti cartacei

I documenti cartacei contenenti **dati personali sensibili** (quali schede relative agli allievi allievi, fogli ore dei dipendenti/collaboratori, certificati di malattia, permessi per visite, etc...) devono essere utilizzati come segue:

- devono essere archiviati in armadi o cassetti chiusi a chiave;
- quelli non utilizzati completamente che non devono essere archiviati, devono essere distrutti o resi illeggibili.

I documenti (o copia degli stessi) non possono, senza specifica autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale dall'azienda.

Il controllo dei documenti stampati o fotocopiati è responsabilità degli INCARICATI al trattamento (N.B.: non dimenticarsi materiale stampato sulle stampanti, fax, fotocopiatrici).

È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria.

Sicurezza dei supporti di memorizzazione

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il TITOLARE nel caso in cui vengano rilevati virus o si verifichino anomalie nel sistema.

I supporti contenenti dati personali devono essere custoditi in archivio, in un'area ad accesso controllato dal personale incaricato o in un armadio/cassetto.

I supporti contenenti dati personali sensibili devono, se possibile, essere marcati con un'opportuna etichetta recante la dicitura *"Contiene dati personali sensibili – DGPR 679/2016"* e devono essere tenuti sotto chiave in armadi o cassetti.

I supporti informatici destinati al riutilizzo (memorie allo stato solido, HDD portatili) devono essere formattati o non devono essere usati per contenere dati personali onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.

Sicurezza del sistema informatico

Il sistema informatico prevede l'assegnazione ad ogni INCARICATO al trattamento di dati personali di:

- una parola chiave riservata conosciuta solamente dal medesimo.

L'INCARICATO deve adottare le necessarie cautele per assicurare la segretezza della password.

L'INCARICATO non deve lasciare incustodito la propria postazione; pertanto deve attivare lo screen saver con la stessa password.

Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione dell'addetto ai sistemi informativi.

Sicurezza dell'accesso a Scolaonline

L'applicativo web prevede l'assegnazione ad ogni utente al trattamento di dati personali di:

- un nome utente
- una parola chiave riservata conosciuta solamente dal medesimo.

L'INCARICATO deve adottare le necessarie cautele per assicurare la segretezza della password.

L'INCARICATO non deve lasciare incustodito la propria postazione; pertanto deve attivare lo screen saver con la stessa password.

PASSWORD (parola chiave segreta)

- per qualunque problema con le PASSWORD rivolgersi al TITOLARE o al personale incaricato
- le PASSWORD possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema;
- le PASSWORD devono essere composte da almeno 8 caratteri;
- la PASSWORD non deve contenere riferimenti agevolmente riconducibili alla persona dell'INCARICATO (quindi non deve contenere l'USER-ID come sua parte componente);
- è necessario procedere alla modifica della PASSWORD, richiesta che viene eseguita automaticamente dal sistema alla scadenza prevista;
- nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi;
- la PASSWORD deve essere immediatamente sostituita, dandone comunicazione alla segreteria, nel caso si sospetti che la stessa abbia perso la segretezza;

Sicurezza contro attacco da virus

Le stazioni informatiche sono protette da software antivirus aggiornato periodicamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Occorre attenersi scrupolosamente alle seguenti regole:

- non disabilitare l'antivirus;
- aggiornare sempre l'antivirus se non aggiornato automaticamente o verificare la data dell'ultimo aggiornamento;
- testare sempre i dispositivi portatili (es. usb drive) provenienti dall'esterno con l'antivirus prima di utilizzarle.

Nel caso il software antivirus rilevi la presenza minacce, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente all'addetto ai sistemi informativi.

5. Regole di utilizzo del sistema informatico

Utilizzo del personal computer (pc)

Il personal computer affidato all'utente è uno strumento di lavoro e deve essere custodito con cura.
Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Il personal computer affidato all'utente permette l'accesso solo attraverso le credenziali di autenticazione già descritte.
Il TITOLARE garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza dei lavoratori.
Non è consentito all'utente

- modificare le caratteristiche impostate sul proprio personal computer, salvo previa autorizzazione esplicita del TITOLARE;
- l'uso di programmi diversi da quelli ufficialmente distribuiti ed installati dal TITOLARE o dal tecnico incaricato;
- installare autonomamente programmi soprattutto se provenienti dall'esterno o da fonte sconosciuta o inaffidabile (salvo previa autorizzazione esplicita dell'addetto ai sistemi informativi) in quanto sussiste il grave pericolo di introdurre virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore;
- il download da internet e l'installazione di software se non autorizzati (anche quelli gratuiti);
- l'esecuzione di file eseguibili (.exe) dei quali non si conosca l'origine.

L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Istituto a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.
Inoltre viene fatto divieto all'utente di:

- riversare sul PC o sulla rete di dati provenienti dall'esterno (sia da dispositivi portatili che dal web) se non preventivamente testati con antivirus aggiornati;
- di modificare le caratteristiche impostate sul proprio personal computer;
- di installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, lettori cd o dvd …), se non con l'autorizzazione espressa del TITOLARE o del tecnico incaricato.

L'utente inoltre deve adottare queste precauzioni:

- il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio (è evidente che lasciare un elaboratore incustodito infatti può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso);
- deve essere attivato lo screen saver con la stessa password usata per l'autenticazione al sistema.

Utilizzo di personal computer portatili

L'utente è responsabile del personal computer portatile assegnatogli dall'Istituto e deve custodirlo con diligenza, sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai pc portatili si applicano le regole di utilizzo previste per quelli connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I personal computer portatili utilizzati all'esterno (convegni, fiere, visite presso la clientela, ecc….), in caso di allontanamento devono essere custoditi in un luogo protetto.
Tali disposizioni si applicano anche nei confronti di INCARICATI esterni quali agenti, collaboratori, ecc.
I portatili che vengono sconnessi dalla rete aziendale non ricevono gli aggiornamenti automatici e pertanto hanno un grado di protezione non allineato con gli standard aziendali. Occorre pertanto porre particolare cura al loro utilizzo e provvedere immediatamente all'aggiornamento dell'antivirus.

Utilizzo dei supporti di memorizzazione
Tutti i supporti rimovibili, contenenti dati sensibili nonché informazioni costituenti know-how aziendale dell'Istituto, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Titolare o un suo incaricato nel caso in cui vengano rilevati virus.
È vietato l'utilizzo di supporti rimovibili personali.

Utilizzo delle unità di rete (dischi su server)
Le disposizioni per il corretto utilizzo sono:
- le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi;
- su queste unità, vengono svolte regolari attività di controllo, amministrazione e back-up;
- le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite;
- è assolutamente proibito entrare nella rete e nei programmi con altri nomi utente;
- il TITOLARE può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà pericolosi per la sicurezza dei dati personali o non inerenti all'attività lavorativa sia sui PC dei dipendenti sia sulle unità di rete;
- costituisce buona regola di condotta la periodica mensile pulizia degli archivi, con cancellazione (o spostamento su unità locali come ad esempio il disco C:) dei files obsoleti o inutili;
- è da evitare un'archiviazione ridondante che non consenta in modo chiaro ed inequivocabile l'identificazione dello stato di revisione di un documento.

Utilizzo delle e-mail
La casella di posta elettronica, assegnata dall'Istituto all'utente, è uno strumento di lavoro.
Si rende noto che i singoli indirizzi e-mail non sono indirizzi personali ma **indirizzi aziendali** che riportano un riferimento al cognome del dipendente ai soli fini di smistamento delle comunicazioni dell'Istituto.
Pertanto ciò che è presente nelle singole caselle di posta non si può ritenere, all'interno della sede aziendale, soggetto alle regole di riservatezza previste dalla legge sulla privacy.
Tale disposizione riguarda sia la posta in uscita sia la posta in entrata.
Si consiglia quindi, nel caso l'indirizzo e-mail sia utilizzato per l'invio dall'esterno di corrispondenza e/o pubblicità non inerente alle attività dell'Istituto, di avvertire la fonte di provenienza.
Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili specialmente se contengono allegati ingombranti.

Esso non è un servizio in tempo reale, ovvero il tempo fra invio e ricezione di un messaggio non è istantaneo e dipende da molti fattori esterni.
L'invio di e-mail con allegati di grandi dimensioni deve essere limitata onde evitare sovraccarico sul server centrale e sulla rete esterna.
È fatto espresso divieto di utilizzare la casella di posta elettronica assegnata per motivi diversi da quelli strettamente legati all'attività lavorativa e quindi per

- l'invio e/o il ricevimento di messaggi estranei al rapporto di lavoro o alle relazioni tra colleghi/Direzione aziendale;
- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o di Sant'Antonio).

È fatto inoltre divieto come misure di sicurezza di:

- aprire posta elettronica proveniente da mittenti sconosciuti o sospetti; se fosse comunque indispensabile l'apertura di tali mail, è consigliabile salvare i file interessati su disco e sottoporli a scansione prima di aprirli.
- aprire allegati caratterizzati da file eseguibili (file .exe), script (file .scr) o altri file sconosciuti (di solito contengono virus)

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o pre-contrattuali per l'azienda deve essere visionata od autorizzata dalla Direzione aziendale, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
La documentazione elettronica che costituisce per l'Istituto "know how" aziendale tecnico o commerciale protetto (tutelato in base all'art. 6 bis del R.D. del 29.06.1939 n.1127), e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.
È possibile utilizzare la "conferma di recapito" per avere la certezza che il messaggio mail sia stato consegnato al server del destinatario, ed utilizzare la "conferma di lettura" per avere certezza dell'avvenuta presa visione del messaggio stesso da parte del destinatario.
Di norma, per qualsivoglia comunicazione ufficiale che riguardi l'Istituto, è obbligatorio avvalersi della P.E.C. di cui si è dotato il medesimo ovvero degli strumenti tradizionali (fax, lettera raccomandata a/r, ecc. …).
Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il TITOLARE mette a disposizione dell'utente apposite funzionalità che consentano di inviare automaticamente in caso di assenze messaggi di risposta che contengano le coordinate di un altro indirizzo e-mail o altre modalità utili di contatto presso l'Istituto.
In caso di assenze programmate, la funzionalità deve essere attivata dall'utente. In caso di assenza non programmata (ad es. per malattia) verrà attivata a cura dell'Istituto.
Una volta conclusosi il rapporto di lavoro/collaborazione tra l'incaricato e l'Istituto, l'indirizzo e-mail associato all'incaricato verrà disattivato e la casella di posta (ed il suo contenuto), al fine di garantire la continuità operativa ed il know-how aziendale, verrà associata all'indirizzo e-mail del nuovo incaricato.

Utilizzo di Internet

Il personal computer abilitato alla navigazione web e all'uso di Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa.

È assolutamente proibita:

- la navigazione in Internet e registrazione a siti per motivi diversi da quelli strettamente legati all'attività lavorativa stessa;
- la partecipazione a forum non professionali;
- la partecipazione a forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames);
- lo scarico di software gratuito (freeware) e a pagamento (shareware) prelevato da siti Internet, se non espressamente autorizzato dal TITOLARE;
- l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione aziendale e con il rispetto delle normali procedure di acquisto.

Il TITOLARE o un suo tecnico incaricato potrà procedere a controlli sulla navigazione finalizzati esclusivamente a garantire l'operatività e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative: es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.

Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre sette giorni. Verranno eseguite eventualmente statistiche anonime sui files di log al fine di aggiornare i filtri di navigazione o per eseguire i controlli graduali specificati nel successivo capitolo 6).

Utilizzo di altri servizi Internet

L'utilizzo di ulteriori servizi forniti da Internet attuali o futuri quali FTP, Newsgroup, Telnet tramite *client* può essere effettuato solo per motivi aziendali e solo su autorizzazione del TITOLARE che provvederà ad attivare le misure di sicurezza adeguate in primo luogo configurando gli strumenti di sicurezza (firewall, proxy, antivirus etc.) già presenti e utilizzati in azienda per i nuovi servizi.

Utilizzo dei telefoni, fax e fotocopiatrici aziendali

Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa.

La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza.

Qualora venisse assegnato all'utente un cellulare aziendale, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Al cellulare aziendale si applicano le medesime regole come sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.

È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

Utilizzo e salvaguardia dei beni aziendali

Ogni dipendente/collaboratore è tenuto a operare con la dovuta cura e diligenza per tutelare i beni aziendali attraverso comportamenti responsabili ed in linea con le procedure operative predisposte per regolamentarne l'utilizzo.

Ognuno è responsabile della protezione delle risorse a lui affidate e ha il dovere d'informare tempestivamente le strutture aziendali preposte circa eventuali eventi dannosi per l'Istituto.
In particolare ogni dipendente/collaboratore:

- è tenuto ad evitare usi impropri di attrezzature (autovetture, telepass, telefoni di rete fissa o mobile, tessera carburante) o quant'altro di proprietà dell'Istituto causando costi indebiti, o danni o comunque in contrasto con gli interessi aziendali;
- è tenuto ad operare sempre nel rispetto delle norme di sicurezza previste dalla Legge e delle procedure interne, allo scopo di prevenire possibili danni a cose, persone o all'ambiente;
- è tenuto ad utilizzare i beni aziendali di qualsiasi tipo e valore secondo il loro corretto uso e nel rispetto della Legge e delle normative interne aziendali;
- è tenuto ad operare al fine di ridurre il rischio di furti, danneggiamenti o altro di beni dell'Istituto.

Tutti beni aziendali sono da utilizzare esclusivamente per scopi connessi all'esercizio dell'attività lavorativa e, comunque, è vietato l'utilizzo o la cessione dei beni stessi da parte di terzi o a favore di terzi.
Si segnala che, il mancato rispetto o la violazione delle regole contenute nel presente Regolamento, è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

6. Sistemi di controlli

Il TITOLARE ha predisposto il proprio sistema informativo e la rete intranet ed internet al fine di utilizzare tali beni aziendali per esclusive esigenze organizzative e/o produttive.
A tal fine, si avvale legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4), di sistemi che consentono indirettamente un controllo a distanza (controlli preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori; e ciò, anche in presenza di attività di controllo discontinue.
In particolare tale attività di controllo potrà essere esercitata nel caso in cui:

- si rilevino anomalie di funzionamento;
- sia a rischio la sicurezza dei citati beni aziendali e/o la sicurezza sul lavoro in generale;
- si rendano necessarie attività di manutenzione (ad esempio aggiornamento sostituzione implementazione di programmi, manutenzione hardware, etc.).

Sarà facoltà della Direzione, tramite addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.
Il TITOLARE dichiara di non utilizzare sistemi hardware e/o software idonei ad effettuare un controllo a distanza dei lavoratori, in particolare mediante:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail e il back-up dei dati;
- la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- la lettura o la registrazione dei caratteri inseriti tramite la tastiera e analogo dispositivo;
- l'analisi occulta del computer portatili affidati in uso.

Il TITOLARE, in merito alla conservazione dei dati, adotta le seguenti procedure.
I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.
In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici è giustificata da una finalità specifica e comprovata e limitata nel

tempo necessario a raggiungerla. Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e avverrà solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità giudiziaria e della Polizia giudiziaria.

In questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità esplicitati.
In caso di anomalie, il TITOLARE o un suo tecnico incaricato effettuerà **controlli anonimi** che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie. In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Osservanza delle disposizioni in materia di Privacy
È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di INCARICATO del trattamento dei dati.

Sanzioni
È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente regolamento.

Aggiornamento e revisione
Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

6. Documenti di riferimento

CODICE	DESCRIZIONE	UBICAZIONE	DURATA CONSERVAZIONE
SQ	INFORMATIVA ALUNNI MAGGIORENNI	SEGRETERIA	Fino al termine del ciclo di studi
SQ	INFORMATIVA FAMIGLIE (ALUNNI MINORI)	SEGRETERIA	Fino al termine del ciclo di studi
SQ	INFORMATIVA TRATTAMENTO DEI DATI PERSONALI	SEGRETERIA	Un anno
SQ	LIBERATORIA CONSENSO INFORMATO	SEGRETERIA	Sempre