ISTITUTO COMPRENSIVO STATALE "Solesino-Stanghella"
Scuola Primaria e Secondaria di I grado Solesino-Granze-Stanghella-BoaraPisani-Vescovana

Viale Papa Giovanni XXIII, 106 - 35047 SOLESINO (PD) - C.M. PDIC854002 - C.F. 82007150285
Segreteria: ☎ 0429-709096 fax 0429-770392 email pdic854002@istruzione.it
pdic854002@pec.istruzione.it dirigenza@icsolesino-stanghella.edu.it www.icsolesino-stanghella.edu.it

REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI DA PARTE DEL PERSONALE DOCENTE

Approvato dal Consiglio di Istituto nella seduta del 10 maggio 2021

INFORMAZIONI DOCUMENTO:

Titolo	Regolamento per l'utilizzo degli strumenti		
Data di emissione	13.01.2021	**Versione**	A513000.07.00 rev. 00

SOMMARIO

1. RIFERIMENTI NORMATIVI

- **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 (Regolamento Generale sulla protezione dei dati) – GPDR;
- **Decreto Legislativo 196/2003** (Codice in materia di protezione dei dati personali) e s.m.i. – Codice della privacy;
- **Lavoro: le linee guida del Garante per posta elettronica e internet**, Garante della protezione dei dati, Gazzetta Ufficiale n. 58 del 10 marzo 2007, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1387522;
- **Misure e accorgimenti prescritti ai Titolari dei Trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema,** Garante della protezione dei dati, Gazzetta Ufficiale n. 300 del 24 dicembre 2008, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499;
- **Legge 20 maggio 1970, n. 300** (Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento) – Statuto dei Lavoratori.

2. PREMESSE E FINALITÀ DEL REGOLAMENTO

L'Istituto mette a disposizione Strumenti - ossia dotazioni hardware e software nonché risorse informatiche/telematiche quali, a titolo esemplificativo, PC, notebook, tablet, smartphone, stampanti, email, software, applicativi, … – quali strumenti di lavoro atti a rendere la prestazione lavorativa/professionale.

Conseguentemente, l'Istituto ha deciso di adottare il presente Regolamento al fine di fornire un quadro preciso di indicazioni per i Lavoratori e gli altri Destinatari (definiti infra) in merito alle corrette modalità di funzionamento degli strumenti sopracitati. Tali indicazioni, infatti, permetteranno di evitare problemi, disservizi, maggiori costi (di manutenzione o altri) nonché di minimizzare rischi/minacce alla sicurezza dei sistemi in uso e/o dei dati in essi contenuti (siano essi dati personali o pertinenti al patrimonio e all'attività dell'Istituto).

L'uso di tali strumenti deve sempre ispirarsi ai principi di diligenza, buona fede e correttezza cui devono costantemente uniformarsi i soggetti che sono autorizzati all'uso degli stessi.

Il Regolamento ha, dunque, il precipuo fine di guidare il comportamento dei Destinatari affinché gli stessi non espongano sé o l'Istituto a sanzioni pecuniarie o penali derivanti da un uso scorretto o illecito degli Strumenti ovvero a conseguenze pregiudizievoli per il patrimonio e/o per immagine dell'Istituto.

Ulteriore fine del presente documento è rappresentato dalla volontà di codesto Istituto di dare attuazione alle disposizioni contenute nel Regolamento UE 2016/679 (GDPR) nonché di allinearsi ai provvedimenti emanati dall'Autorità Garante della Protezione dei Dati (cfr. le linee guida sopracitate) al fine di garantire sia la protezione dei dati personali trattati mediante gli Strumenti sia la salvaguardia del patrimonio informativo dell'Istituto.

Ne consegue che, ai fini del presente Regolamento, per "dati" deve intendersi l'insieme delle informazioni di cui i Destinatari vengano a conoscenza e di cui devono garantire riservatezza e segretezza (a prescindere dalla

circostanza che si tratti o meno di dati personali). Ogni dato nell'accezione sopradescritta, infatti, è da considerarsi riservato.

Al contrario, non rientra tra le finalità del presente Regolamento il controllo a distanza e/o in forma occulta delle attività, delle abitudini o delle opinioni dei lavoratori.

Nel rispetto, dunque, delle previsioni di cui allo Statuto dei Lavoratori (cfr. art. 4 e 8 dello stesso) il Regolamento è atto a disciplinare le modalità di raccolta dei dati tramite gli Strumenti nonché l'eventuale potere disciplinare in capo a codesto Istituto in casi di uso improprio o non autorizzato dei sopracitati Strumenti.

Le prescrizioni di seguito previste integrano e specificano le istruzioni già impartite agli autorizzati ai sensi del GDPR e le informazioni già fornite agli interessati ai sensi dell'art. 13 del medesimo Regolamento Europeo, anche in ordine ai possibili controlli e alle conseguenze disciplinari in caso di violazione delle stesse ai sensi dell'art. 4, co. 3, dello Statuto dei Lavoratori.

3. CAMPO DI APPLICAZIONE

Il Regolamento si applica a tutti i soggetti che, a qualsiasi titolo, utilizzano gli Strumenti (di seguito denominati anche "Destinatari" o "Utenti"). A titolo esemplificativo e non esaustivo, esso si applica:

- ✓ ai lavoratori subordinati, a prescindere dalla durata del rapporto, dall'orario, dal ruolo, dalla funzione ricoperta o dalla modalità in cui viene resa la prestazione (per es. smart working);
- ✓ ai collaboratori dell'Istituto indipendentemente dal rapporto contrattuale in essere;
- ✓ altri soggetti che si trovino in possesso di specifiche credenziali di autenticazione per accedere alla rete informatica dell'Istituto o che, comunque, utilizzino altri Strumenti, anche in ipotesi di uso solo temporaneo.

4. PRINCIPI GENERALI E RISERVATEZZA DELLE COMUNICAZIONI

L'Istituto si ispira ai principi espressi dal GDPR con riferimento ai dati personali. Nello specifico:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- principio di necessità: i sistemi ed i programmi sono configurati riducendo al minimo l´utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite; i dati personali sono trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento;
- principio di necessità: i sistemi ed i programmi sono configurati riducendo al minimo l´utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite. I dati personali sono trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi;
- principio di pertinenza e non eccedenza: i trattamenti sono effettuati per finalità determinate, esplicite e legittime. L'Istituto tratta i dati *"nella misura meno invasiva possibile; le attività di monitoraggio sono svolte solo da soggetti preposti e sono mirate sull'area di rischio, tenendo conto della normativa sulla*

protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza" (Linee Guida del Garante per posta elettronica e internet)*;*

- principio di trasparenza: le informazioni e le comunicazioni relative al trattamento di tali dati personali devono essere facilmente accessibili e comprensibili utilizzando un linguaggio semplice e chiaro.

5. NORME DI COMPORTAMENTO GENERALI DA ADOTTARE NELL'USO DEGLI STRUMENTI

L'Utente è consapevole che gli Strumenti sono di proprietà dell'Istituto e sono messi a disposizione al fine di permettere allo stesso di rendere la prestazione. Conseguentemente, unicamente a tale fine tali Strumenti possono essere utilizzati.

I Destinatari del presente Regolamento devono improntare il proprio comportamento in relazione agli Strumenti attenendosi ai principi di diligenza, correttezza e liceità. In particolare:

- Gli Strumenti non possono essere ceduti a terzi, a qualsivoglia titolo, nemmeno parzialmente (es. sim, auricolari, pc, …) né possono essere utilizzati da soggetti diversi dall'Utente assegnatario;
- Gli Strumenti devono essere correttamente custoditi e mantenuti in buono stato. L'Utente, dunque, è tenuto a segnalare eventuali malfunzionamenti/ disservizi/ comportamenti anomali/ danneggiamenti/ aggiornamenti ed a richiedere al DSGA che si provveda con i necessari interventi;
- Quando tali Strumenti dovranno essere restituiti – a prescindere dalle motivazioni che tale restituzione hanno comportato per es. cessazione del rapporto, cambio di mansione con relativa modifica degli Strumenti, … - essi dovranno essere integri ed in buono stato conservativo;
- In caso di furto, smarrimento o danneggiamento degli Strumenti l'Utente dovrà darne pronta comunicazione all'Istituto, fornendo alla stessa ogni utile chiarimento e/o informazione;
- Qualora il Destinatario debba allontanarsi dagli Strumenti, in particolare in caso di apparecchi non fissi, dovrà assicurarsi che gli stessi si trovino in locali chiusi a chiave o siano comunque custoditi in luogo idoneo (es. armadio chiuso a chiave);
- Una diligente custodia degli Strumenti andrà effettuata anche qualora l'Utente sia autorizzato ad utilizzarli al di fuori dei locali dell'Istituto;
- L'utilizzo di memorie di massa esterne (es. chiavette USB, hard disk, …) è consentito solo nella misura per cui ciò risulti strettamente necessario al raggiungimento di una specifica finalità; in ogni caso, il docente sarà direttamente responsabile del contenuto delle stesse e dovrà aver cura di custodirle in modo da preservare gli eventuali dati personali ivi contenuti;
- È vietato utilizzare servizi di web drive non esplicitamente autorizzati dal Titolare per il salvataggio di dati personali;
- Non è consentito modificare la configurazione hardware/software degli Strumenti forniti;
- È vietato installare modem, schede di rete cablate o wireless o qualsiasi altro dispositivo di connessione, salvo espressa autorizzazione;
- Se lo Strumento è dotato di scheda modem o altro dispositivo di trasmissione dati, essi andranno disabilitati laddove si sia connessi alla rete dell'Istituto;
- Si ricorda inoltre che la funzione logout, laddove presente, deve essere utilizzata al termine di ogni sessione di lavoro/utilizzo specifico. In particolare il logout dal registro elettronico, account di posta e piattaforme cloud deve essere sempre effettuato al termine del loro utilizzo;
- È vietato lasciare traccia nei dispositivi dell'Istituto di file contenenti dati personali, se non espressamente autorizzati;
- I seguenti comportamenti risultano poi proibiti, salvo espressa autorizzazione del Titolare: installare e/o utilizzare dispositivi hardware esterni per uso non professionale/lavorativo; installare/copiare software/ programmi/ dispositivi; eliminare software/programmi/dispositivi installati per configurazione predefinita dal Titolare; connettere gli Strumenti a reti esterne;

- È vietata qualsiasi attività volta a compromettere o anche solo eludere i meccanismi di protezione adottati dal Titolare.

6. ASSEGNAZIONE, GESTIONE E REVOCA DELLE CREDENZIALI DI ACCESSO

Le credenziali consistono in un codice identificativo dell'Utente (username o user id) ed una password.
I destinatari sono responsabili di tutte le attività svolte attraverso l'uso delle proprie credenziali. Pertanto, la password è personale e riservata e dovrà essere conservata con la massima cura e diligenza, senza comunicarla a terzi o divulgarla. Ne consegue che è vietato:

- trascrivere le proprie credenziali/password su fogli, biglietti, post-it o altri supporti;
- inserire le credenziali in messaggi di posta elettronica (siano essi in chiaro o crittografati) né possono essere salvate su altri strumenti/documenti informatici (es file excel/word, …) che non siano protetti a loro volta da apposite credenziali;
- digitare la propria password in presenza di soggetti che possano vedere la tastiera;
- utilizzare credenziali diverse da quelle ricevute in quanto assegnate in virtù del ruolo ricoperto e alla luce del rapporto intercorrente con l'Istituto.

La stessa dovrà avere adeguate caratteristiche di robustezza:

- Numero minimo di caratteri: 8;
- Deve essere composta da caratteri alfabetici sia minuscoli che maiuscoli, da caratteri numerici e da simboli speciali (es. !?/()*…);
- Non deve contenere riferimenti agevolmente riconducibili all'Utente come il nome, la data di nascita, il numero di matricola, nomi o date relative a familiari, codice fiscale, ecc.

Qualora l'Utente ritenesse che la password abbia perso di riservatezza dovrà provvedere a chiederne la sostituzione all'Amministratore di Sistema. Nel caso in cui, invece, la password venisse smarrita, l'Utente dovrà provvedere a effettuare un recupero della password per il tramite dell'Amministratore di Sistema.

Periodicamente viene effettuata dall'Amministratore di Sistema una verifica delle utenze esistenti e dei rispettivi profili di accesso.

I log di accesso sono registrati e possono essere oggetto di controllo dall'Istituto, per il tramite dell'Amministratore di sistema, per esigenze di cui al paragrafo 22.

Potranno dunque effettuarsi controlli come previsto del presente Regolamento.

Le informazioni così raccolte sono utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del presente Regolamento, che costituisce adeguata informazione sulle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del GDPR.

7. OPERAZIONI A PROTEZIONE DELLA POSTAZIONE DI LAVORO

Con riferimento alla postazione di lavoro, il destinatario dovrà osservare le norme di seguito previste.

- É necessario accertarsi che persone non autorizzate non possano prendere visione della schermata del dispositivo in uso- e ciò soprattutto quando l'utente inserisce le proprie credenziali - né di documenti/supporti contenenti dati personali;
- Al termine dell'attività condotta, l'utente garantirà che la postazione fisica utilizzata sia priva di materiali o documenti contenenti dati personali;
- Raccogliere gli stampati e i documenti non più necessari e provvedere al loro smaltimento, ossia mediante distruzione degli stessi per il tramite di distruggi documenti o altri strumenti idonei a ridurre in piccoli pezzi gli stessi.

8. MEMORIZZAZIONE E PROTEZIONE DEI DATI

L'integrità e la disponibilità dei dati (inteso quali informazioni e dati dell'Istituto, compresi i dati personali trattati dal Titolare) è garantita unicamente qualora gli stessi vengano memorizzati nell'ambito dei sistemi improntati appositamente dal Titolare.

Ne consegue che i Destinatari dovranno provvedere a trasferire nei pertinenti archivi/cartelle tutti i dati presenti negli Strumenti e/o nelle memorie fisse o removibili autorizzate nonché servizi cloud.

Si ricorda, peraltro, che le informazioni memorizzate possono essere unicamente quelle necessarie e sufficienti all'attività lavorativa / professionale ed è, dunque, buona pratica provvedere alla pulizia di file obsoleti, inutili o duplici almeno con cadenza semestrale.

Qualora sia necessario avere copia di tali dati, la stessa andrà salvata solo su supporti autorizzati dal Titolare i quali dovranno essere conservati in luoghi protetti (es. armadi e cassettiere chiusi a chiave). Inoltre, quando gli stessi andranno restituiti al Titolare (anche in ipotesi di sostituzione o distruzione del supporto) o consegnati a terzi, il Destinatario dovrà avere l'accortezza di verificarne il contenuto nonché provvedere a cancellare dati eventualmente non più necessari o non pertinenti.

Qualora vi sia un malfunzionamento dei sistemi o un errata configurazione / uso degli stessi, per qualsivoglia causa occorsi, che comportino che il Destinatario venga a conoscenza di dati che non è autorizzato a trattare (si pensi al ricevimento di una mail indirizzata ad altri), lo stesso dovrà esimersi dal consultare il documento e segnalare l'accaduto al proprio Responsabile affinché siano adottate le opportune misure anche in concerto con l'Amministratore di Sistema.

9. UTILIZZO DI COMPUTER E COMPUTER PORTATILI

I computer ed i computer portatili rappresentano uno dei principali Strumenti di cui si avvale il Titolare.

Oltre alle disposizioni che riguardano gli Strumenti in generale oppure una loro specifica modalità di utilizzo (es. uso della posta elettronica, …), si ricorda che trovano applicazione le seguenti regole di comportamento:

- Non è consentita l'attivazione di password di accensione (BIOS) senza previa autorizzazione dell'Amministratore di Sistema;
- È obbligatorio consentire, al primo momento disponibile, l'installazione degli aggiornamenti di sistema che vengano proposti automaticamente;
- È vietato il loro uso per l'acquisizione/riproduzione/condivisione illegale di materiale protetto da copyright.

I log relativi all'utilizzo di tali Strumenti – reperibili nella memoria dello strumento stesso, sul server o sul router - ed i file con essi trattati possono essere oggetto di controllo da parte del Titolare, attraverso l'Amministratore di Sistema, per esigenze di cui al paragrafo 22. Tali controlli avverranno secondo quanto previsto nel presente Regolamento. Le informazioni così raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto, compreso il rispetto del presente Regolamento, che costituisce idonea informazione ai sensi del GDPR.

10. UTILIZZO DI INTERNET

L'Istituto consente l'utilizzo di Internet mediante dispositivi pre-autorizzati e/o per mezzo di identificazione con nome utente e password, laddove presente.

Tutti i Destinatari devono rispettare le seguenti regole di comportamento:

- l'utilizzo del collegamento d'Istituto al web deve essere effettuato unicamente per scopi connessi all'attività lavorativa e, in ogni caso, nel rispetto dei principi di liceità, diligenza e correttezza nonché del rapporto in essere tra l'Utente e l'Istituto;
- la navigazione è consentita per i siti che contengono informazioni utili all'attività lavorativa ovvero forniscono idoneo supporto informativo professionale;
- l'Istituto può prevedere, mediante appositi strumenti di "filtro", il blocco di siti/categorie di siti ritenuti pericolosi o estranei alle attività condotte dall'Istituto. In caso di blocco accidentale di siti d'interesse, l'Utente potrà contattare l'Amministratore di Sistema per lo sblocco;
- in ogni caso, non è consentito all'utente navigare o memorizzare file con contenuto o di natura contraria alle norme di legge, oltraggiosa, violenta, pornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione o appartenenza politica;
- l'Utente non dovrà installare, nei dispositivi dell'Istituto, software gratuiti o in licenza d'uso, di qualsivoglia natura, che non siano autorizzati dal Dirigente Scolastico;
- è proibito violare la Legge sul Diritto d'Autore e/o le norme a tutela della proprietà industriale, in particolare, scaricando o condividendo illecitamente contenuti di qualsiasi genere (video, testi, immagini, brani, …) protetti dalla sopracitata normativa;
- i file di provenienza esterna o incerta, quand'anche ricollegabili all'attività lavorativa, devono sempre essere sottoposti al controllo dell'antivirus. In caso di dubbio sull'integrità o sulla sicurezza del file l'Utente è invitato a prendere contatti con il personale addetto/referente transazione digitale;
- i Destinatari si impegnano a non interferire con il buon funzionamento dei sistemi informatici e di rete dell'Istituto;
- l'Utente deve segnalare tempestivamente al personale addetto e/o all'Amministratore di Sistema la presenza di attività sospetta sui propri sistemi o sulla rete;
- per motivi tecnici e di buon funzionamento del sistema informatico è buona regola, salvo comprovate esigenze, non accedere a risorse web che impegnino in modo rilevante la banda;
- per permettere una comoda interazione tra colleghi, l'Istituto può mettere a disposizione un sistema di messaggistica istantanea mediante i soli strumenti autorizzati dall'Amministratore di Sistema. Anche per tali strumenti possono essere effettuati i controlli di cui al presente Regolamento.

Nel caso di cessazione del rapporto di lavoro ovvero della collaborazione tra l'Istituto e l'Utente, per qualsiasi motivo intervenuta, copia del traffico internet verrà conservata sul server centrale o sui backup dell'Istituto entro i termini previsti dal presente regolamento e/o dalla retention policy d'Istituto, salvo che vi siano elementi che inducano l'Istituto a ritenere necessario un periodo di conservazione più ampio (ad es. per finalità di difesa in giudizio) anche in seguito ad un eventuale valutazione di impatto ai sensi dell'art. 35 del GDPR.

L'Istituto, per il tramite dell'Amministratore di sistema, non controlla in modo sistematico le pagine web né effettua controlli automatici sui dati di navigazione.

Tuttavia, l'Istituto, per il tramite dell'Amministratore del Sistema, registra per un massimo di 6 mesi i dati di navigazione (file di log del traffico web) ai fini di cui al paragrafo 22.

Tali controlli avverranno secondo quanto previsto nel presente Regolamento. Le informazioni così raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto, compreso il rispetto del presente Regolamento, che costituisce idonea informazione ai sensi del GDPR.

11. UTILIZZO DELL'INFRASTRUTTURA DI RETE

L'Istituto dispone di una rete cui possono accedere, mediante credenziali strettamente personali, unicamente gli Utenti a ciò abilitati.

L'accesso alla rete permette all'Utente di accedere alle cartelle sul server per potervi salvare i files rilevanti rispetto all'attività prestata, organizzati per area/ufficio oppure per criteri logici (area tematica, progetto, cliente, …).

Nell'utilizzo delle risorse di rete dovranno essere seguite le seguenti norme:

- le cartelle di rete possono ospitare esclusivamente contenuti professionali. Conseguentemente, non potranno essere salvati né sul server né sui dispositivi in dotazione, file di contenuto o natura personale. Qualora tale materiale dovesse essere reperito dall'Amministratore sul server, quest'ultimo provvederà ai sensi del di quanto previsto *infra* con riferimento ai controlli alla rimozione dello stesso, impregiudicata ogni ulteriore responsabilità civile, penale o disciplinare;
- al di fuori delle risorse di cui al server, l'Amministratore non effettua alcun controllo regolare e non vengono effettuati backup sulle altre risorse (ad es. cartella "desktop" dell'Utente, dispositivi di memorizzazione locale ad uso esclusivo, …). È responsabilità del singolo utente provvedere all'immediato salvataggio dei file di interesse nelle cartelle di rete di pertinenza;
- senza il consenso dell'Istituto, è fatto divieto di salvare / trasferire documenti elettronici dai sistemi e strumenti dell'Istituto in dispositivi esterni;
- è possibile accedere alle risorse di rete anche mediante la rete senza fili (wifi), presente all'interno delle sedi lavorative e mediante autenticazione con credenziali;
- i servizi di connettività wireless di ogni tipo (salvo il wifi in caso di collegamento tramite tale modalità alla rete d'Istituto) disponibili sui dispositivi utilizzati devono essere sempre disabilitati in particolar modo laddove si sia connessi alla rete d'Istituto;
- l'Istituto può permettere agli Utenti di accedere alla rete dell'Istituto dall'esterno. Tale accesso potrà avvenire mediante VPN, ossia un canale criptato e privato verso la rete interna, oppure tramite altre modalità congrue. Le richieste di abilitazione a tale modalità di accesso dovranno essere effettuate con le modalità di cui al presente Regolamento.

In ogni caso, l'Amministratore di Sistema si riserva la facoltà di negare o interrompere l'accesso alla rete qualora esso avvenga mediante strumenti non adeguatamente aggiornati o protetti.

Inoltre, l'Amministratore di Sistema ed il personale addetto potranno provvedere alla rimozione di qualsivoglia file/applicazione che riterranno pericolosa per la sicurezza della rete dell'Istituto.

I log di accesso al sistema o all'intranet sono registrati e possono essere oggetto di controllo dall'Istituto, per il tramite dell'Amministratore di sistema, per esigenze di cui al paragrafo 22.

Tali controlli avverranno secondo quanto previsto nel presente Regolamento. Le informazioni così raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto, compreso il rispetto del presente Regolamento, che costituisce idonea informazione ai sensi del GDPR.

12. UTILIZZO DELLA POSTA ELETTRONICA

La casella di posta elettronica assegnata all'Utente è uno strumento di lavoro di cui gli assegnatari sono responsabili sia sotto il profilo della garanzia della riservatezza delle credenziali di accesso sia sotto il profilo del corretto utilizzo.

È fatto divieto di utilizzare la casella di posta per motivi diversi da quelli strettamente legati all'attività lavorativa e/o che esulino dall'espletamento delle mansioni affidate a ciascun Utente.

A titolo esemplificativo, l'Utente **non potrà**:

- inviare o ricevere allegati contenenti foto/filmati, brani musicali (o link a contenuti di tale genere) che non siano legati all'attività prestata;

- inviare o ricevere messaggi personali o per la partecipazione a dibattiti, aste online, forum, mailing list, newsletter, salvo diversa esplicita autorizzazione da parte del Responsabile area/ufficio;
- partecipare alle cosiddette catene di "sant'Antonio";
- creare, archiviare o spedire messaggi pubblicitari o promozionali in nessun modo connessi con lo svolgimento della prioria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto;
- inviare o memorizzare messaggi o file di natura oltraggiosa, violenta, volgare e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione, appartenenza sindacale e/o politica;
- utilizzare la casella di posta dell'Istituto per ragioni e/o finalità personali.

Inoltre, per una corretta fruizione del servizio di posta elettronica dell'Istituto devono essere rispettate le seguenti regole:

- per garantire la sicurezza della rete è necessario prestare particolare attenzione alla posta ricevuta. In caso di mail da mittenti sconosciuti o messaggi insoliti, di dubbia autenticità o di provenienza e/o con contenuti non attinenti all'attività svolta dall'Utente ovvero con contenuti anomali è necessario verificare la sorgente/intestazione del messaggio e, in caso di dubbio, contattare il personale addetto. Ciò per evitare di essere infettati da virus/malware e/o di essere vittima di phishing. A seguito della verifica con individuazione di possibili minacce si dovrà procedere alla cancellazione dei messaggi senza aprirli;
- non dovranno essere aperti file con estensioni diverse da quelle comunemente in uso e/o con nomi sospetti o altre anomalie;
- qualora, in allegato ad una mail, vi dovessero essere file eseguibili (.exe) ovvero file di archivio compresso (.zip, .rar, .tar, …) è necessario accertarsi preventivamente del loro contenuto verificando il mittente (eventualmente tramite contatto diretto con lo stesso);
- è obbligatorio controllare i file ricevuti in allegato alla mail per accertarne la sicurezza contattando il mittente. Inoltre, in casi di dubbio o in ipotesi di cui al punto che precede, rivolgersi sempre al personale addetto;
- non bisogna cliccare su link di provenienza dubbia o incerta senza averli verificati con il mittente nonché con il personale addetto;
- nell'invio di allegati utilizzare solo formati comuni (.doc, .xls, .pdf,…) e accertarsi che non vengano superate le dimensioni massime consentite sia per il mittente (dimensioni massime 10 MB) che per il destinatario;
- nel caso in cui fosse necessario inviare allegati "pesanti" è opportuno ricorrere prima alla compressione degli stessi in formato .zip o equivalente. Se anche in tale modo il file risultasse eccessivamente pesante dovrà essere contattato il personale addetto;
- la posta elettronica non deve essere utilizzata per ricevere, inviare o memorizzare materiale che violi le norme sul diritto d'autore o sulla proprietà industriale;
- La casella deve essere mantenuta in ordine, cancellando messaggi e documenti inutili o la cui conservazione non è necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, prediligendo, il salvataggio dell'allegato nelle condivisioni. Inoltre, con cadenza mensile, l'Utente deve provvedere ad archiviare le mail di rilevanza per l'attività del Titolare nelle opportune cartelle del Server dell'Istituto;
- è possibile utilizzare le funzionalità di "conferma di recapito" e "conferma di lettura";
- nell'eventualità di natura eccezionale che sia necessario inviare messaggi contenenti allegati con dati personali è obbligatorio che tali file vengano preventivamente resi inintelligibili tramite cifratura con apposito software (archiviazione e compressione con password). La password per cifrare il documento andrà comunicata al destinatario della comunicazione attraverso un canale diverso dalla mail e in nessun

caso unitamente ai dati criptati stessi. Tali informazioni andranno, inoltre, inviate unicamente a destinatari legittimati a riceverle;

- la diffusione massiva di messaggi di posta elettronica deve essere effettuata unicamente per motivi inerenti al servizio e su autorizzazione dell'Istituto. I destinatari dovranno essere inseriti in copia conoscenza nascosta (Ccn);
- è vietato inviare messaggi in nome e per conto di altro soggetto, salvo una sua espressa autorizzazione;
- i messaggi in entrata vengono sistematicamente analizzati per la ricerca di virus e malware e per l'eliminazione di spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario viene avvisato mediante messaggio specifico;
- poiché è stato stabilito un limite massimo delle dimensioni della casella di posta, all'utente sarà notificato del raggiungimento di tale limite. Superato lo stesso, non sarà possibile inviare nuovi messaggi e l'Utente dovrà provvedere alle operazioni necessarie per ripristinarne la funzionalità (cancellazione e/o archiviazione della posta);

Si informano gli Utenti che, in caso di richiesta da parte elle Autorità competenti (Guardia di Finanza, Autorità giudiziaria, …), le mail memorizzate sui server dell'Istituto potrebbero essere rese note e consegnate alle stesse.

Nel caso di cessazione del rapporto di lavoro ovvero della collaborazione tra l'Istituto e l'Utente, per qualsiasi motivo intervenuta, la mail affidata all'Utente verrà disattivata immediatamente. Il sistema, in ogni caso, potrà generare una risposta automatica informando il mittente della disattivazione e invitando quest'ultimo a rivolgersi ad altro dipendente/funzione dell'Istituto.

Una volta disattivato l'account di posta, copia dei messaggi verrà conservata sul server centrale o sui backup dell'Istituto entro i termini previsti dalla retention policy dell'Istituto, salvo che vi siano elementi che inducano l'Istituto a ritenere necessario un periodo di conservazione più ampio (ad es. per finalità di difesa in giudizio) anche in seguito ad un eventuale valutazione di impatto ai sensi dell'art. 35 del GDPR.

L'Istituto, per il tramite dell'Amministratore di sistema, non controlla in modo sistematico il flusso di comunicazioni mail né è dotata di sistemi di lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, ultronei rispetto a quanto tecnicamente necessario per svolgere il servizio di email.

Tuttavia, per esigenze di cui al punto 22, l'Istituto, per il tramite dell'Amministratore del Sistema, può accedere all'account di posta prendendo visione dei messaggi, salvando o cancellando file come previsto dal presente Regolamento.

Tali controlli avverranno secondo quanto previsto nel presente Regolamento. Le informazioni così raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto, compreso il rispetto del presente Regolamento, che costituisce idonea informazione ai sensi del GDPR.

13. USO PERSONALE

L'uso personale di internet o di servizi di web mail privati durante l'orario di lavoro e/o mediante gli Strumenti dell'Istituto è consentito solo occasionalmente ed in ipotesi eccezionali e, in ogni caso, con modi, tempi e durata tali da non arrecare pregiudizio all'organizzazione del Titolare o all'attività lavorativa.

14. SOFTWARE

L'Istituto mette a disposizione degli Utenti anche taluni software, per i quali vigono le seguenti regole di comportamento:

- L'Istituto acquista le licenze d'uso dei software e dunque è soggetta a limitazioni nel loro utilizzo. Ne consegue che le medesime limitazioni valgono anche nei confronti dei Destinatari;
- I Destinatari non potranno riprodurre i software, salvo ragioni di salvataggio (copie di backup opportunamente documentate);
- All'infuori dei software messi a disposizione dell'Istituto, gli Utenti non potranno utilizzarne altri, salvo espressa autorizzazione. Tale divieto vige in particolare per tutti quei software atti ad intercettare, falsificare o alterare il contenuto di documenti informatici (ad es. programmi di password recovery, cracking, sniffing, …);
- Qualora l'Utente dovesse venire a conoscenza di qualsivoglia criticità derivante dalla configurazione o da difetti intrinsechi dei software dovrà darne tempestiva comunicazione al personale incaricato;
- Non dovranno essere modificati gli standard di configurazione dei software installati.

15. ANTIVIRUS

Gli strumenti, laddove tecnicamente possibile, verranno dotati di software antivirus adeguatamente configurati ed aggiornati. Ogni Utente deve comunque tenere comportamenti tali da minimizzare i rischi di attacchi informatici a danno del sistema informatico dell'Istituto.

Ogni dispositivo di provenienza esterna, per il cui utilizzo l'Utente deve essere già stato autorizzato, nonché i files eseguibili o contenenti software vengono verificati dall'antivirus.

Nel caso in cui l'antivirus rilevasse la presenza di un virus, l'Utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnare il dispositivo e segnalare l'accaduto al proprio responsabile che a sua volta si rivolgerà all'Amministratore di Sistema.

Un'eventuale segnalazione dovrà, inoltre, essere effettuata qualora il Destinatario accerti la non presenza o il mancato aggiornamento dell'antivirus.

16. UTILIZZO DI TELEFONO FISSO/ CELLULARE/ SMARTPHONE/ TABLET/ FAX

Per quanto riguarda il telefono fisso/ cellulare/ smartphone/ tablet/ fax, non sono consentite comunicazioni a carattere personale o non strettamente inerenti all'attività lavorativa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentita solo nel caso di comprovata necessità ed urgenza. Inoltre, non sono consentite chiamate a numeri a pagamento, salvo espressa autorizzazione del proprio referente/responsabile.

Peraltro, per cellulare/smartphone/tablet, strumenti dei quali l'assegnatario sarà responsabile con riferimento al loro utilizzo e alla loro custodia, vigono le seguenti regole di comportamento, oltre a quelle già previste nei paragrafi sopra laddove compatibili (cfr. per es. uso strumenti elettronici, posta elettronica e navigazione Internet):

- proteggere tutti i dati presenti nel dispositivo anche mediante *"pin code"* (o analoghi strumenti), sistemi di blocco automatico dello schermo e cifratura;
- non scaricare/installare applicazioni non preventivamente richieste al proprio referente/responsabile ed autorizzate dal personale addetto.

Rimane inteso che, in ipotesi di comprovato rischio per i dati presenti su cellulari/ smartphone/ tablet (es. furto, smarrimento, …) l'Istituto si riserva la facoltà di intervenire anche da remoto sugli stessi. A tale fine, gli strumenti dovranno essere configurati in modo da consentire la ricezione di una richiesta remota di cancellazione dei dati e dei contenuti.

Per tali Strumenti potranno essere effettuati i controlli di cui al presente Regolamento. Le informazioni così raccolte sono, inoltre, utilizzabili a tutti i fini connessi al rapporto, compreso il rispetto del presente Regolamento, che costituisce idonea informazione ai sensi del GDPR.

17. UTILIZZO DI SISTEMI DI RIPRODUZIONE

L'uso di sistemi di riproduzione quali stampanti e scanner è consentito esclusivamente per motivi connessi all'esecuzione della prestazione lavorativa/professionale, anche nel rispetto dei principi di economia e di salvaguardia dell'ambiente.

La produzione di copie cartacee o informatiche di documenti, soprattutto se aventi natura riservata o contenenti dati personali, deve essere giustificata da una concreta necessità e l'Utente dovrà presidiare il processo di stampa/scansione al fine di impedire che terzi non autorizzati possano conoscere le sopracitate informazioni. Conseguentemente, sarà cura dell'Utente provvedere a recuperare immediatamente le stampe presso la fotocopiatrice e cancellare i file contenenti dati personali/riservati qualora siano accessibili a soggetti non autorizzati.

Si ricorda di prediligere le stampanti di rete condivise nonché stampare, laddove possibile, in bianco/nero e fronte/retro di modo da ridurre i materiali di consumo ed i costi.

Il loro utilizzo per fini personali può essere ammesso unicamente per ipotesi eccezionali e delimitate temporalmente e quantitativamente senza che ne venga incisa l'attività generale e l'organizzazione dell'apparato del Titolare. In tali ipotesi sarà cura del soggetto interessato circostanziare la richiesta al proprio Responsabile.

18. SISTEMI IN CLOUD

Utilizzare un servizio in cloud per memorizzare dati può esporre il Titolare a potenziali rischi. Ne consegue che è vietato il loro utilizzo eccettuato il caso in cui sia il Titolare stesso ad approvare taluni sistemi cloud.

19. ASSISTENZA DEGLI UTENTI E MANUTENZIONE

L'Amministratore di Sistema può accedere ai dispositivi sia direttamente sia attraverso software di accesso remoto per i seguenti motivi:

a. Verificare e risolvere problemi sistemici ed applicativi su segnalazione dell'Utente;
b. Verificare il corretto funzionamento dei singoli dispositivi qualora venissero rilevati problemi nella rete;
c. Evadere richieste di aggiornamento software o manutenzione preventiva;
d. Effettuare i controlli previsti dal presente Regolamento.

Per le ipotesi *a*, *b* e *c*, qualora l'effettuazione dell'intervento renda necessario l'accesso alle aree personali dell'Utente, l'Amministratore dovrà ottenerne il previo consenso. Diversamente, l'intervento tecnico che si limiti ad accedere ad aree non riservate all'Utente potrà effettuarsi senza il consenso di quest'ultimo.

Nel caso in cui soggetti terzi (es. fornitori) debbano accedere in teleassistenza ai dispositivi degli utenti, dovrà essere ottenuta per il primo accesso l'autorizzazione dell'Amministratore di Sistema che verificherà le modalità di intervento. Le richieste successive, invece, potranno essere gestite in autonomia dall'Utente purché avvengano con le modalità autorizzate dall'Amministratore.

Rimane inteso che gli interventi in teleassistenza di terzi richiedono sempre la presenza dell'Utente o dell'Amministratore di Sistema per impedire comportamenti non conformi al presente Regolamento.

Inoltre, qualora si rendesse necessario permettere l'accesso da remoto alla rete dell'Istituto al personale di imprese fornitrici per l'adempimento di obblighi contrattuali in essere, l'Amministratore di Sistema è autorizzato, previa richiesta scritta da parte del Titolare, a rilasciare i profili autorizzativi. Rimane inteso che, in tali casi, al fornitore verrà data copia del presente Regolamento al quale quest'ultimo dovrà attenersi.

20. CONTROLLI SUGLI STRUMENTI (AD INTEGRAZIONE DELL'INFORMATIVA PRIVACY GIÀ CONSEGNATA)

L'uso degli Strumenti, come analiticamente precisato nel Regolamento d'Istituto sul loro utilizzo, può lasciare traccia di talune informazioni eventualmente contenenti dati personali dell'Utente.

In tale ambito rientrano anche i cosiddetti files di log ossia una serie di informazioni aggregate dei sistemi preposti alla gestione di internet, posta elettronica e rete interna dell'Istituto, che contengono dati relativi alle operazioni effettuate dagli utenti in un certo ambito (ad es. sistema, applicazioni, data base, …). I files di log contengono tipicamente: data e ora dell'operazione effettuata, utente, tipologia dell'operazione e dati associati alla stessa.

Il Titolare si riserva la facoltà di effettuare controlli, nei limiti di quanto consentito dalle norme legali e contrattuali, sugli Strumenti per:

1. Verificare l'integrità e la sicurezza dei sistemi;
2. Per la manutenzione degli Strumenti o altri motivi tecnici (es. aggiornamento, sostituzione, implementazione di programmi, …);
3. La tutela del patrimonio, compreso il patrimonio informativo;
4. Constatare utilizzi indebiti e/o non conformi degli Strumenti come definiti nel Regolamento anche su eventuale segnalazione di terzi o dell'Autorità Giudiziaria;
5. Comprovate esigenze produttive o organizzative.

Il datore di lavoro, infatti, può avvalersi, nel rispetto dell'art. 4 co. 2 dello Statuto dei Lavoratori, di sistemi che indirettamente consentono il controllo dei lavoratori purché nel rispetto delle procedure di informazione nei confronti dei lavoratori anche in base alla normativa privacy vigente.

In particolare, verranno rispettati i seguenti principi nel condurre i suddetti controlli:

- Proporzionalità: l'estensione del controllo dovrà avere un carattere adeguato, pertinente e non eccessivo;
- Trasparenza: il presente Regolamento ha il precipuo obbiettivo di informare gli Utenti sui diritti ed i doveri delle parti;
- Pertinenza e non eccedenza: non avverrà alcuna interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori né vi sarà alcun controllo prolungato, costante o indiscriminato.

Si segnala che le informazioni derivanti dai controlli condotti potranno essere utilizzabili a tutti i fini connessi al rapporto di lavoro. Ciò in quanto l'informativa ai lavoratori e il Regolamento sull'uso degli Strumenti costituiscono idonea informazione circa le modalità d'uso degli Strumenti e dell'effettuazione dei controlli nel rispetto, in ogni caso, della normativa vigente.

Il mancato rispetto o la violazione delle regole contenute nel Regolamento sugli Strumenti è perseguibile con provvedimenti disciplinari, così come disciplinati dal Ccnl ed altresì con le azioni civili e penali qualora si ravvisino gli estremi per integrare tali responsabilità.

CONTROLLO PER LE FINALITÀ 1,2,3,4

Qualora risulti necessario accedere agli Strumenti e alle relative informazioni per le finalità di cui ai punti 1, 2, 3, 4 il Titolare, per il tramite dell'Amministratore di Sistema, si atterrà al processo di seguito riportato, con gli opportuni adeguamenti in base allo specifico Strumento oggetto di controllo.

- I controlli, ove possibile, verranno effettuati preventivamente su informazioni appartenenti a gruppi collettivi di Destinatari e su dati aggregati tramite analisi statistiche, anche generali. Si sottolinea come gli stessi non verranno compiuti in modo prolungato, costante o indiscriminato;
- Avviso generico a tutti i dipendenti, o ad una specifica area/reparto, della presenza di comportamenti anomali e richiamo all'esigenza di attenersi ai compiti assegnati e alle istruzioni impartite;
- Dopo almeno 7 giorni ed in caso di persistenza del comportamento anomalo, l'Istituto potrà autorizzare l'Amministratore di Sistema ad effettuare il controllo ossia ad accedere alle informazioni contenute negli Strumenti, con possibilità di rilevare siti web visitati, files trattati, software installati, statistiche sull'uso, …;
- Tale attività andrà effettuata in forma anonima;
- Si potrà effettuare un controllo su base individuale unicamente in caso di richiesta da parte dell'Autorità Giudiziaria, quando si verifichi un evento dannoso o una situazione di pericolo imminente ovvero quando i controlli di cui ai punti precedenti non hanno condotto alla risoluzione dell'anomalia;
- L' accesso potrà avvenire o tramite le credenziali dell'Amministratore di Sistema o, in caso di controllo su base individuale, mediante la creazione di nuove credenziali (che dovranno essere sostituite dall'Utente al primo accesso);
- Qualora sussista un grave ed imminente rischio rispetto alle finalità per le quali il controllo è condotto, l'Istituto, unitamente all'Amministratore di Sistema, potrà attivarsi per intervenire immediatamente con un controllo su base individuale, senza operare dunque con una gradualità dell'azione di controllo. Rimane inteso che, in tale evenienza, l'Istituto e l'Amministratore di Sistema avranno cura di precisare le motivazioni che hanno condotto ad effettuare tale scelta operativa;
- Redazione di un verbale che riassuma i passaggi precedenti e le motivazioni addotte per effettuare l'accesso.

CONTROLLO PER LA FINALITÀ 5

Qualora risulti necessario accedere agli Strumenti e alle relative informazioni per la finalità di cui al punto 5, il Titolare, per il tramite dell'Amministratore di Sistema, si atterrà al processo di seguito riportato, con gli opportuni adeguamenti in base allo specifico Strumento oggetto di controllo.

Si precisa che tale tipo di accesso è consentito unicamente quando concorrono i seguenti presupposti:

- assenza improvvisa o prolungata del dipendente; e
- improrogabili necessità legate all'attività lavorativa.

In tali ipotesi il Titolare si atterrà alla seguente procedura:

- L'Istituto dovrà redigere documento scritto che comprovi le necessità produttive e/o organizzative e delimiti, per quanto possibile, la natura e specie delle risorse coinvolte;
- L'Interessato è messo in grado di delegare (cfr. modulo allegato) un altro soggetto operante all'interno della Struttura del datore di lavoro (fiduciario). Tale soggetto si occuperà di verificare il contenuto delle risorse coinvolte e di inoltrare all'Istituto quello ritenuto rilevante per i fini di cui alla richiesta;
- La nomina del fiduciario deve avvenire per iscritto e la richiesta di accedere alla casella di posta dovrà essere effettuata dal Responsabile dell'ufficio/area del soggetto assente mediante richiesta scritta indirizzata al fiduciario;
- Nel caso in cui il lavoratore non abbia provveduto a indicare alcun Fiduciario, ovvero quest'ultimo non sia a sua volta reperibile, verrà dato incarico all'Amministratore di Sistema affinché acceda alle risorse informative necessarie. Tale accesso potrà avvenire o tramite le credenziali dell'Amministratore di Sistema o mediante la creazione di nuove credenziali (che dovranno essere sostituite dall'Utente al primo accesso).
- Dell'accesso, inoltre, verrà redatto un verbale che verrà controfirmato dall'Amministratore di Sistema e dal fiduciario ed inviato al soggetto assente.

21. CONSERVAZIONE DEI DATI

I Dati relativi ai files di log verranno conservati per un periodo di 6 mesi. Nel caso in cui l'esercizio del diritto di difesa o una specifica richiesta dell'Autorità dovesse rendere necessario un prolungamento del tempo di conservazione, esso verrà effettuato limitatamente al soddisfacimento di tali necessità.

Il contenuto dei dispositivi di memorizzazione degli strumenti, delle cartelle del server, degli account di posta elettronica, saranno conservati sul server centrale/backup secondo la politica dell'Istituto.

22. ISTRUZIONI IN CASO DI CESSAZIONE DEL RAPPORTO DI LAVORO O DI COLLABORAZIONE

In caso di cessazione del rapporto di lavoro/collaborazione ovvero in tutti i casi in cui l'utente è chiamato a riconsegnare gli strumenti, la restituzione dovrà avvenire senza eliminare alcun dato dell'Istituto e mantenendo il dato stesso leggibile. Rimane inteso che, prima della riconsegna, il destinatario dovrà provvedere a eliminare qualsiasi dato personale a sé riferibile.

I dati dell'Istituto sopracitati non potranno essere conservati, duplicati, comunicati o diffusi dal Destinatario. Viceversa, gli stessi, verranno conservati in base alla policy interna da parte dell'Istituto.

23. SOCIAL MEDIA

L'eventuale utilizzo di canali social da parte dell'Istituto verrà gestito e organizzato esclusivamente da quest'ultimo sulla base di apposito Regolamento.

Ciò non toglie che, pur nel rispetto della libertà di espressione dei singoli utenti che collaborino con l'Istituto, si debba considerare che gli stessi potrebbero essere identificati dai fruitori dei social quali soggetti alle dipendenze di codesta Istituto. Ne consegue che gli Utenti sono chiamati a osservare un comportamento corretto e rispettoso.

Nello specifico, il personale ed i collaboratori sono chiamati ad attenersi alle seguenti regole:

- qualora volessero rendere pubblico il loro rapporto alle dipendenze dell'Istituto sarà necessario che il soggetto indichi nel proprio profilo che le opinioni espresse all'interno del social sono puramente personali e non impegnano in alcun modo l'Istituto;
- non possono essere divulgate, mediante i canali social, informazioni riservate, quali la corrispondenza interna, informazioni di terze parti (a titolo esemplificativo non esaustivo istituzioni, utenti, etc…) o informazioni su attività lavorative, servizi, progetti e documenti non ancora resi pubblici, decisioni da assumere e provvedimenti relativi a procedimenti in corso, prima che siano stati ufficialmente deliberati e/o comunicati formalmente alle parti;
- possono essere liberamente condivisi sui profili personali i contenuti (od un rimando agli stessi) pubblicati nella pagina istituzionale dell'Istituto;
- fermo restando il corretto esercizio delle libertà sindacali e del diritto di critica, non devono essere diffusi o trasmessi messaggi o dichiarazioni ingiuriose, minatorie o offensive nei confronti dell'Istituto;
- non possono essere postati contenuti multimediali che riprendano i locali dell'ente, il personale o i clienti dell'Istituto senza l'esplicita autorizzazione delle persone coinvolte;
- deve essere rispettata la riservatezza dei colleghi evitando, conseguentemente, di pubblicare riferimenti alle attività lavorative svolte, salvo l'ipotesi in cui le stesse non siano di dominio pubblico.

L'interazione con i canali social in ogni caso è severamente vietata durante l'orario lavorativo.

24. DISPOSITIVI PERSONALI

L'utilizzo di dispositivi personali da parte dei docenti è consentito.

Resta inteso che i file contenenti dati personali dovranno essere archiviati unicamente presso sistemi messi a disposizione dall'Istituto (es. cloud, registro elettronico).

25. SANZIONI

Il mancato rispetto o la violazione delle regole contenute nel Regolamento sugli Strumenti è perseguibile con provvedimenti disciplinari, così come disciplinati dal Ccnl ed altresì con le azioni civili e penali qualora si ravvisino gli estremi per integrare tali responsabilità.

26. NORME FINALI

Il presente Regolamento entrerà in vigore con la Sua approvazione da parte dell'organo competente e farà parte integrante del Regolamento Privacy dell'Istituto.

Con la sua entrata in vigore tutte le disposizioni precedentemente adottate in materia si intendono sostituite, qualora incompatibili o difformi, da quanto previsto dal Regolamento.

Esso verrà pubblicato, a cura dell'Istituto, mediante invio per posta elettronica a tutti gli Utenti provvisti di email nonché mediante pubblicazione sul sito istituzionale. Inoltre, esso verrà affisso nei luoghi di lavoro ai sensi dell'art. 7 dello Statuto dei Lavoratori.

Tutti gli Utenti possono proporre integrazioni/modifiche motivate al presente Regolamento.

ALLEGATO 1: Informativa privacy per gli utenti degli strumenti

Informativa privacy per gli Utenti degli Strumenti

Egregio Sig.re / Gentile Sig.ra, ai sensi dell'art. 13 del Regolamento UE 2016/679 (GDPR), il trattamento dei Suoi dati personali sarà improntato ai principi di correttezza, liceità, trasparenza e di tutela della Sua riservatezza e dei Suoi diritti. Pertanto, è gradito fornirle le seguenti informazioni.

Titolare del Trattamento

IC "Solesino-Stanghella", con sede in Viale Papa Giovanni XXIII 106, 35047 Solesino (Padova), tel. 0429 709096, e-mail pdic854002@istruzione.it, PEC pdic854002@pec.istruzione.it, in persona del Suo legale rappresentante pro tempore.

Responsabile della Protezione dei Dati (DPO)

tel. 049 0998416, e-mail dpo@robyone.net, PEC dpo.robyone@ronepec.it

Tipologia di dati raccolti

Dati personali relativi all'utilizzo del sistema informativo e degli Strumenti.

Finalità

1. *Gestire e garantire l'utilizzo e la funzionalità degli Strumenti assegnati;*
2. *Effettuare i controlli di cui al Regolamento sugli Strumenti con lo scopo di garantire l'integrità e la sicurezza dei sistemi, la manutenzione degli Strumenti, la tutela del patrimonio dell'istituto, compreso il patrimonio informativo; di constatare utilizzi indebiti e/o non conformi degli Strumenti; di soddisfare comprovate esigenze produttive e organizzative.*

Base giuridica

Per le finalità sopracitate il trattamento è necessario al fine di eseguire un contratto di cui l'Utente è parte nonché per il perseguimento del legittimo interesse del Titolare o di Terzi, a condizione che non prevalgano interessi, diritti o libertà fondamentali dell'interessato (art. 6, parag. 1, lett. b) e f) del GDPR).

Destinatari dei dati

I dati potranno essere comunicati alle seguenti categorie di soggetti: soggetti incaricati della gestione del personale nell'ambito di rapporti di assistenza e consulenza; soggetti incaricati della tenuta dei dati informatici, della manutenzione hardware/software; soggetti che forniscono servizi per la gestione del sistema informativo del Titolare e delle reti di telecomunicazioni; legali incaricati della tutela del Titolare; autorità competenti per adempimenti di obblighi derivanti dalla legge e/o da disposizioni di organi pubblici, in particolare l'autorità giudiziaria nell'esercizio dei propri compiti giurisdizionali.

Conservazione

I dati del dipendente verranno conservati per il tempo minimo necessario alla loro funzione, nel rispetto del principio di minimizzazione del trattamento dei dati imposto dall'art. 5 par. 1 lett. c del GDPR. I Dati relativi ai files di log verranno conservati per un periodo di 6 mesi.

Obbligatorietà fornitura dei dati, motivazione e conseguenze mancata comunicazione

Il conferimento dei dati è obbligatorio. In mancanza non sarà possibile l'utilizzo degli strumenti assegnati.

Modalità di trattamento

I dati saranno trattati da persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare. Eventuali trattamenti da effettuare in esterno, per attività specifiche non eseguibili all'interno, vengono affidati a soggetti di comprovata affidabilità all'uopo nominati.

Diritti degli interessati

In qualsiasi momento, l'interessato può esercitare il diritto di opposizione al trattamento dei dati che lo riguardano (art. 21 del GDPR).

Inoltre, lo stesso potrà avere accesso ai propri dati personali (art. 15 del GDPR), ottenerne la rettifica o la cancellazione, la limitazione del trattamento (art. 16, 17 e 18 del GDPR), la portabilità (art. 20 del GDPR).

Lei potrà esercitare i sopradescritti diritti contattando il Titolare o il Responsabile della Protezione dei Dati.

Potrà, infine, proporre reclamo all'autorità di controllo (Garante Privacy) (artt. 15, par. 1, lett. f , e 77 del GDPR).

ALLEGATO 2: Informativa sui controlli

Informativa sui controlli sugli Strumenti utilizzati per rendere la prestazione.

L'uso degli Strumenti, come analiticamente precisato nel Regolamento d'Istituto sul loro utilizzo, può lasciare traccia di talune informazioni eventualmente contenenti dati personali dell'Utente.

In tale ambito rientrano anche i cosiddetti file di log ossia una serie di informazioni aggregate dei sistemi preposti alla gestione di internet, posta elettronica e rete interna dell'Istituto, che contengono dati relativi alle operazioni effettuate dagli utenti in un certo ambito (ad es. sistema, applicazioni, data base, ...). I file di log contengono tipicamente: data e ora dell'operazione effettuata, utente, tipologia dell'operazione e dati associati alla stessa.

Il Titolare si riserva la facoltà di effettuare controlli, nei limiti di quanto consentito dalle norme legali e contrattuali, sugli Strumenti per:

1. *Verificare l'integrità e la sicurezza dei sistemi;*
2. *La manutenzione degli Strumenti o altri motivi tecnici (es. aggiornamento, sostituzione, implementazione di programmi, ...);*
3. *La tutela del patrimonio, compreso il patrimonio informativo;*
4. *Constatare utilizzi indebiti e/o non conformi degli Strumenti come definiti nel Regolamento anche su eventuale segnalazione di terzi o dell'Autorità Giudiziaria;*
5. *Comprovate esigenze produttive o organizzative.*

Il datore di lavoro, infatti, può avvalersi, nel rispetto dell'art. 4 co. 2 dello Statuto dei Lavoratori, di sistemi che indirettamente consentono il controllo dei lavoratori purché nel rispetto delle procedure di informazione nei confronti dei lavoratori anche in base alla normativa privacy vigente.

In particolare, verranno rispettati i seguenti principi nel condurre i suddetti controlli:

- *Proporzionalità: l'estensione del controllo dovrà avere un carattere adeguato, pertinente e non eccessivo;*
- *Trasparenza: il presente Regolamento ha il precipuo obbiettivo di informare gli utenti sui diritti ed i doveri delle parti;*
- *Pertinenza e non eccedenza: non avverrà alcuna interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori né vi sarà alcun controllo prolungato, costante o indiscriminato.*

Si segnala che le informazioni derivanti dai controlli condotti potranno essere utilizzabili a tutti i fini connessi al rapporto di lavoro. Ciò in quanto l'informativa ai lavoratori e il Regolamento sull'uso degli Strumenti costituiscono idonea informazione circa le modalità d'uso degli Strumenti e dell'effettuazione dei controlli nel rispetto, in ogni caso, della normativa vigente.

Il mancato rispetto o la violazione delle regole contenute nel Regolamento sugli Strumenti è perseguibile con provvedimenti disciplinari, così come disciplinati dal Ccnl ed altresì con le azioni civili e penali qualora si ravvisino gli estremi per integrare tali responsabilità.

<u>CONTROLLO PER LE FINALITÀ 1,2,3,4</u>

Qualora risulti necessario accedere agli Strumenti e alle relative informazioni per le finalità di cui ai punti 1, 2, 3, 4 il Titolare, per il tramite dell'Amministratore di Sistema, si atterrà al processo di seguito riportato, con gli opportuni adeguamenti in base allo specifico Strumento oggetto di controllo.

- *I controlli, ove possibile, verranno effettuati preventivamente su informazioni appartenenti a gruppi collettivi di Destinatari e su dati aggregati tramite analisi statistiche, anche generali. Si sottolinea come gli stessi non verranno compiuti in modo prolungato, costante o indiscriminato;*
- *Avviso generico a tutti i dipendenti, o ad una specifica area/reparto, della presenza di comportamenti anomali e richiamo all'esigenza di attenersi ai compiti assegnati e alle istruzioni impartite;*
- *Dopo almeno 7 giorni ed in caso di persistenza del comportamento anomalo, l'Istituto potrà autorizzare l'Amministratore di Sistema ad effettuare il controllo ossia ad accedere alle informazioni contenute negli Strumenti, con possibilità di rilevare siti web visitati, files trattati, software installati, statistiche sull'uso, ...*
- *Tale attività andrà effettuata in forma anonima;*

- *Si potrà effettuare un controllo su base individuale unicamente in caso di richiesta da parte dell'Autorità Giudiziaria, quando si verifichi un evento dannoso o una situazione di pericolo imminente ovvero quando i controlli di cui ai punti precedenti non hanno condotto alla risoluzione dell'anomalia;*
- *L' accesso potrà avvenire o tramite le credenziali dell'Amministratore di Sistema o, in caso di controllo su base individuale, mediante la creazione di nuove credenziali (che dovranno essere sostituite dall'Utente al primo accesso);*
- *Qualora sussista un grave ed imminente rischio rispetto alle finalità per le quali il controllo è condotto, l'Istituto, unitamente all'Amministratore di Sistema, potrà attivarsi per intervenire immediatamente con un controllo su base individuale, senza operare dunque con una gradualità dell'azione di controllo. Rimane inteso che, in tale evenienza, l'Istituto e l'Amministratore di Sistema avranno cura di precisare le motivazioni che hanno condotto ad effettuare tale scelta operativa;*
- *Redazione di un verbale che riassuma i passaggi precedenti e le motivazioni addotte per effettuare l'accesso.*

CONTROLLO PER LA FINALITÀ 5

Qualora risulti necessario accedere agli Strumenti e alle relative informazioni per la finalità di cui al punto 5, il Titolare, per il tramite dell'Amministratore di Sistema, si atterrà al processo di seguito riportato, con gli opportuni adeguamenti in base allo specifico Strumento oggetto di controllo.

Si precisa che tale tipo di accesso è consentito unicamente quando concorrono i seguenti presupposti:

- *assenza improvvisa o prolungata del dipendente; e*
- *improrogabili necessità legate all'attività lavorativa.*

In tali ipotesi il Titolare si atterrà alla seguente procedura:

- *Il Dirigente Scolastico o il DSGA dovrà redigere documento scritto che comprovi le necessità produttive e/o organizzative e delimiti, per quanto possibile, la natura e specie delle risorse coinvolte;*
- *L'Interessato è messo in grado di delegare (cfr. modulo allegato) un altro soggetto operante all'interno della Struttura del datore di lavoro (fiduciario). Tale soggetto si occuperà di verificare il contenuto delle risorse coinvolte e di inoltrare all'Istituto quello ritenuto rilevante per i fini di cui alla richiesta;*
- *La nomina del fiduciario deve avvenire per iscritto e la richiesta di accedere alla casella di posta dovrà essere effettuata dal Responsabile dell'ufficio/area del soggetto assente mediante richiesta scritta indirizzata al fiduciario;*
- *Nel caso in cui il lavoratore non abbia provveduto a indicare alcun Fiduciario, ovvero quest'ultimo non sia a sua volta reperibile, verrà dato incarico all'Amministratore di Sistema affinché acceda alle risorse informative necessarie. Tale accesso potrà avvenire o tramite le credenziali dell'Amministratore di Sistema o mediante la creazione di nuove credenziali (che dovranno essere sostituite dall'Utente al primo accesso).*
- *Dell'accesso, inoltre, verrà redatto un verbale che verrà controfirmato.*

ALLEGATO 3: Modulo Nomina Fiduciario

Nomina di soggetto fiduciario

Il/La sottoscritto/a _____ codice fiscale _____ in qualità di utente di _____

DELEGA

in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, i seguenti soggetti

nome e cognome _____ codice fiscale _____

nome e cognome _____ codice fiscale _____

nome e cognome _____ codice fiscale _____

a verificare il contenuto degli strumenti da me utilizzati e ad inoltrare all'Istituto quello ritenuto rilevante ai fini di cui alla richiesta.

Data _____

Firma _____