ISTITUTO COMPRENSIVO DI REVELLO
V.le Umberto I, 33 - 12036 REVELLO (CN) - Tel 0175 257176
cnic834002@istruzione.it - cnic834002@pec.istruzione.it - www.icrevello.edu.it
c.f. 94033220040 codice IPA istsc_cnic834002 codice univoco UFJQTE

REGOLAMENTO

per la gestione dei dati mediante strumenti informatici e cartacei

Al fine dell'attuazione del GDPR 2016/679 e del decreto legislativo 30 giugno 2003, n. 196

Sommario

CAPO I – PRINCIPI

Art. 1 – Introduzione, Definizioni e Finalità

Il presente Regolamento ha l'obiettivo di garantire il corretto trattamento dei dati di cui l'Istituto Comprensivo è titolare, nel rispetto della normativa vigente i materia di privacy, sia che si tratti di dati processati con modalità digitale che gestiti in forma cartacea.

Ha altresì l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione da parte degli utenti assegnatari (dipendenti, collaboratori ecc.) al fine di tutelare i beni dell'Istituto ed evitare condotte inconsapevoli o scorrette che potrebbero esporre questa Pubblica Amministrazione a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.

L'insieme delle norme comportamentali da adottare è ispirato ai principi di diligenza, informazione, correttezza nell'ambito dei rapporti di lavoro e inoltre finalizzato a prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti a essi attribuiti dall'ordinamento giuridico italiano.

Art. 2 – Ambito di applicazione

Il presente Regolamento si applica a ogni utente autorizzato al trattamento dati (art. 4 Regolamento UE 2016/679 e art. 2 quaterdecies D.Lgs. 2003/196) e/o assegnatario di beni e risorse informatiche di proprietà dell'Isituto ovvero utilizzatore di servizi e risorse informative dell'ente.

Per **utente** pertanto si intende, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore, consulente, fornitore o altro che in modo continuativo non occasionale operi all'interno della struttura aziendale utilizzandone beni e servizi informatici.

Per **ente** si intende, l'Istituto Comprensivo di Revello, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

Art. 3 – Titolarità dei beni e delle risorse informatiche

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni dell'Istituto rientranti nel patrimonio statale e sono da considerarsi di esclusiva proprietà dell'ente.

Ciò considerato, il loro utilizzo è consentito solo per finalità di adempimento delle mansioni lavorative affidate a ciascun utente in base al rapporto in essere, ovvero per gli scopi professionali afferenti l'attività svolta per l'ente, e comunque per l'esclusivo perseguimento degli obiettivi aziendali.

A tal fine si precisa sin d'ora che qualsivoglia dato o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà dell'ente sarà dallo stesso considerato come avente natura aziendale e non riservata.

Art. 4 – Responsabilità personale dell'utente

Ogni utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dall'ente nonché dei relativi dati trattati le finalità di lavoro.

A tal fine ogni utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l'ente e per quanto di propria competenza, è tenuto a tutelare il patrimonio informatico da utilizzi impropri o non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è e rimane sempre quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse della scuola.

Ogni utente è tenuto a operare a tutela della sicurezza informatica, in relazione al proprio ruolo e alle mansioni in concreto svolte, riportando al proprio responsabile organizzativo diretto (Dirigente scolastico o Direttore SGA) e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente Regolamento. Sono vietati comportamenti che possano creare un qualsiasi danno, anche di immagine, all'ente.

Art. 5 – Controlli

L'ente esclude la configurabilità di forme di controllo aventi direttamente a oggetto l'attività lavorativa dell'utente, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, statuto dei lavoratori).

Gli eventuali controlli previsti sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento (UE) 2016/679, alla legge n. 300/1970 (Statuto dei lavoratori) e ai provvedimenti emanati dall'Autorità Garante (in particolare Provvedimento del 1 marzo 2007).

In particolare non si esclude che si utilizzino sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro. Per tali evenienze sarà onere dell'ente sottoporre tali forme di controllo all'accordo con le RSU. In difetto di accordo e su istanza dell'ente è l'ispettorato del lavoro a indicare le modalità per l'uso di tali impianti.

I controlli posti in essere saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati.

L'ente, riservandosi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici dell'Istituto (artt. 2086, 2087 e 2104 c.c.), agirà in base al principio della gradualità. In attuazione di tale principio:

- I controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intero istituto ovvero a singole aree lavorative;
- Nel caso in cui si dovessero riscontrare violazioni del presente Regolamento, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e

diligenza, verrà diffuso un avviso generalizzato o circoscritto all'area o struttura lavorativa interessata, relativo all'uso anomalo degli strumenti informatici aziendali, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite;

- In caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

L'ente titolare non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.

Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:

- La lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- La memorizzazione sistematica delle pagine internet visualizzate da ciascun utente, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;
- La lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;
- L'analisi dei dispositivi per l'accesso alla rete internet.

Capo II — MISURE ORGANIZZATIVE

Art. 6 – Amministratori di sistema

L'ente conferisce all'amministratore di sistema il compito di sovrintendere ai beni e alle risorse informatiche aziendali. È compito dell'amministratore di sistema:

- Gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'ente;
- Gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
- Monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- Creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- Rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché si tratti di attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;

- Provvedere alla sicurezza informatica dei sistemi informativi aziendali;
- Utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata a un utente in caso di prolungata assenza, non rintracciabilità o impedimento dello stesso.

Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di soggetto autorizzato al trattamento dei dati personali (o *designato*) all'interno dell'ente e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

Per la parte relativa alla strumentazione assegnata alla didattica e la gestione degli accessi al wifi per docenti e studenti tale ruolo è assunto dall'animatore digitale e viene indicato nelle funzioni elencate nell'atto di nomina.

Per la parte relativa alla segreteria tale funzione è assegnata al DSGA, che può delegare, con specifico atto, il tecnico informatico o un assistente amministravo con particolari competenze o il tecnico esterno incaricato della gestione della rete.

Deve essere redatto un elenco completo degli amministratori di sistema, contenente tutti i dati rilevanti, aggiornato con cadenza annuale ovvero ogni volta che si rilevino modifiche.

Art. 7 – Assegnazione degli account e gestione delle password

7.1 – Creazione e Gestione degli Account

Al personale sono assegnati account e password per lo svolgimento della propria attività lavorativa e in particolare:

- Al personale di segreteria, è assegnato:
    - un account utente per accedere alle singole postazioni lavorative e al server della segreteria.
    - Un account utente per accedere alla piattaforma di gestione del flusso documentale del programma di segreteria
    - eventuali account per accedere a piattaforme specifiche per la gestione delle procedure di ufficio, su incarico del DSGA o del Dirigente Scolastico
- Al personale docente e ATA è assegnato:
    - un account per accedere al Registro Elettronico
    - un account per accedere alla piattaforma di Istituto
    - eventuali altri account per accesso a risorse specifiche della scuola

Gli account utenti vengono creati dagli amministratori di sistema e sono personali,

cioè associati univocamente alla persona assegnataria. Ogni utente è responsabile dell'utilizzo del proprio account utente.

L'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione",(username e password), comunicate all'utente dall'amministratore di sistema che le genera con modalità tali da garantirne la segretezza.Le credenziali di autenticazione costituiscono dati da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi, anche a soggetti in posizione apicale all'interno dell'ente.

Se l'utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, è tenuto a modificare immediatamente la password e a segnalare la violazione all'amministratore del sistema nonché al responsabile privacy di riferimento.

In caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive aziendali o per la sicurezza e operatività delle risorse informatiche, l'ente si riserva la facoltà di accedere a qualsiasi dotazione o apparato assegnato in uso all'utente per mezzo dell'intervento dell'amministratore di sistema.

7.2 – Gestione e Utilizzo delle Password

A seguito della prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'utente ha il compito di modificare al primo utilizzo la propria password procedendo allo stesso modo ogni 6 mesi e, nel caso di trattamento di categorie particolari di dati personali (art. 9 GDPR - (origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, 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) o relativi a condanne penali e reati o a connesse misure di sicurezza (art. 10 GDPR), almeno ogni 3 mesi.

L'utente, nel definire il valore della password, deve rispettare, se non diversamente richiesto dalla piattaforma specifica, le seguenti regole:

- Utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, ecc.), di cui almeno uno numerico;
- Inserire almeno un carattere maiuscolo, un carattere minuscolo, un numero o un carattere non alfanumerico tipo "@#$£$%...";
- Evitare di includere parti del nome, cognome o comunque elementi a lui agevolmente riconducibili;
- Evitare l'utilizzo di password comuni o prevedibili;

L'utente deve proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

È fatto divieto di scrivere la password su post-it o altri supporti in quanto compromette in maniera pressoché totale le misure di sicurezza previste.

È fatto altresì divieto la memorizzazione delle proprie password all'interno dei device della scuola.

7.3 – Cessazione degli Account

In caso di interruzione del rapporto di lavoro con l'utente, le credenziali di autenticazione verranno disabilitate entro un periodo massimo di 30 (trenta) giorni da quella data; entro 90 (novanta) giorni, invece, si disporrà la definitiva e totale cancellazione dell'account utente.

7.4 – Dispositivi privi di accesso con account e password - didattica

I dispositivi a disposizione del docente collocati in classe e in aula docenti non sono configurati con accesso tramite account e password per le attività offline. Tali computer sono dotati di un programma di pulizia che elimina i file creati durante la sessione nel momento in cui si spegne il pc.

Pertanto su tali supporti non deve essere salvato o archiviato alcun file contenente dati personali e in particolare quelli indicati all'art.9 del Reg.UE 2016/679 (origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, 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).

Tutti i dispositivi utilizzati dagli allievi per lo svolgimento delle attività didattiche devono essere configurati in modo da garantire l'accesso alla rete wifi solo tramite autenticazione con account e password dello studente, da attivare a cura del docente o dell'amministratore di sistema solo durante le attività didattiche che richiedono l'uso di internet.

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 8 – Postazioni di lavoro

Per postazione di lavoro si intende il complesso unitario di personal computer (di seguito pc), notebook, tablet, smartphone, accessori, periferiche e ogni altro dispositivo (*device*) concesso in utilizzo all'utente. L'assegnatario di tali beni e strumenti informatici aziendali ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile.

Al fine di disciplinare un corretto utilizzo di tali beni l'ente ha adottato le seguenti regole tecniche:

- Ogni pc, notebook (accessori e periferiche incluse), tablet, smartphone o altro dispositivo (*device*), sia esso acquistato, noleggiato o affidato in locazione, rimane di esclusiva proprietà dell'ente ed è concesso all'utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività svolta.
- È dovere di ogni utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente.
- Il pc e gli altri dispositivi di cui sopra devono essere utilizzati con hardware. Non è consentito rimuovere, danneggiare o asportare componenti hardware;
- Tutti i device devono essere utilizzati con software autorizzati dall'ente. Non è consentito modificare la configurazione hardware e software del proprio dispositivo (*device*), se non previa esplicita autorizzazione dell'ente (per le modalità operative fare riferimento a quanto riportato all'art. 20 – Comunicazioni) che la esegue per mezzo dell'amministratore del sistema;
- L'ente si riserva la facoltà di rimuovere d'ufficio e senza alcun preavviso qualsiasi elemento hardware o software la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.
- L'utente deve segnalare con la massima tempestività all'amministratore di sistema o al proprio responsabile di riferimento eventuali guasti e problematiche tecniche rilevati o il cattivo funzionamento delle apparecchiature.
- Al termine delle attività tutti i device destinati alle attività didattiche devono essere riposti nelle aule informatiche opportunamente chiuse.
- È fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici dell'Istituto a soggetti terzi, nonché portarli all'esterno dell'edificio scolastico.

Al fine di garantire la sicurezza dei dati trattati si sottolinea l'obbligo di:

- non lasciate incustodite le postazioni con le sessioni utenti attive.

- bloccare tastiera e schermo con un programma salvaschermo (*screensaver*) protetto da password o effettuare il log-out dalla sessione quando l'utente si allontana dalla propria postazione di lavoro deve.
- Spegnere il PC al termine del lavoro. Per quanto concerne la gestione dei computer e degli altri dispositivi portatili, l'utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti;eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus nonché sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore del sistemaNon caricare o inserire all'interno del computer o di altri dispositivi portatili qualsiasi dato personale non attinente con l'attività lavorativa svolta.

In ogni caso, al fine di evitare o almeno ridurre al minimo la possibile circolazione di dati personali sul medesimo apparecchio, gli utenti devono cancellare tutti quelli eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione.

Art. 9 – Device di proprietà dell'utente

Gli apparecchi di proprietà personale dell'utente quali computer portatili, telefoni cellulari, smartphone, agende palmari, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali e qualsiasi altro dispositivo non potranno essere collegati ai computer o alle reti informatiche dell'Istituto salvo preventiva autorizzazione scritta dell'ente.

Tali apparecchi di proprietà dell'utente non potranno altresì essere utilizzati per lo svolgimento di attività che richiedano il trattamento di dati personali.

Non è autorizzato alcun accesso a internet sui dispositivi dell'ente utilizzando la connessione mobile di un device di proprietà dell'utente (hotspot o tethering).

Art. 10 – Software

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno ottenere espressa autorizzazione dell'ente (per le modalità operative fare riferimento a quanto riportato all'art. 20 – Comunicazioni) per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria, ad esempio *freeware* o *shareware*.

Il personale deve prestare attenzione ad alcuni aspetti fondamentali che ciascun utente è tenuto a osservare per un corretto utilizzo del software

- Le licenze d'uso del software sono acquistate da vari fornitori esterni. L'utente è pertanto soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga ai diritti concessigli. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei rispettivi contratti di licenza.
- Non è consentito eseguire il download o l'upload di software non autorizzato.

- Considerato quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi soggette alle sanzioni previste dalla legge che comprendono il risarcimento del danno, il pagamento di multe e anche la reclusione.
- La duplicazione illegale del software non è giustificabile e non è tollerata, costituisce violazione del presente Regolamento ed espone alle sanzioni disciplinari e amministrative previste dalla normativa.

Art. 11 – Dispositivi di memoria portatili

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, files, o documenti esternamente al computer: cd-rom, dvd, pen-drive USB, riproduttori musicali mp3, fotocamere digitali, dischi rigidi esterni, ecc.

L'utilizzo di tali supporti risponde alle direttive di seguito riportate:

- non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dall'ente (per le modalità operative fare riferimento a quanto riportato all'art. 20 – Comunicazioni);
- l'Istituto fornisce supporti mobili per la custodia di file contenenti dati particolari (art.9 del GDPR: origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, 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).
- è onere dell'utente custodire tali supporti contenenti categorie particolari di dati (art. 9 GDPR) o dati relativi a condanne penali e a reati (art. 10 GDPR) in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato o distrutto;

Se autorizzati in base alle procedure previste, una volta connessi all'infrastruttura informatica dell'ente, i dispositivi saranno soggetti (ove ciò sia compatibile) al presente Regolamento.

Art. 12 – Stampanti e fotocopiatrici

L'utilizzo di tali strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte dell'ente.

Quando si inviano documenti contenenti dati personali o informazioni riservate su una stampante condivisa è richiesta una particolare attenzione; ciò al fine di evitare che persone non autorizzate possano venire a conoscenza del contenuto della stampa. Bisogna evitare quindi di lasciare le stampe incustodite e ritirare immediatamente le copie appena stampate.

Art. 13 – Strumenti di fonia mobile o di connettività in mobilità

A seconda del ruolo o della funzione del singolo utente, l'ente rende disponibili impianti di telefonia fissa e mobile e inoltre dispositivi quali smartphone e tablet che consentono di usufruire sia della navigazione in internet tramite rete dati che del servizio di telefonia tramite rete mobile.

Le specifiche relative ai limiti entro cui l'utente potrà utilizzare tali strumenti saranno indicate in una nota consegnata unitamente al dispositivo. L'utente dovrà attenersi ai suddetti limiti e in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.

Come per qualsiasi altra dotazione della scuola, il dispositivo mobile rappresenta un bene aziendale concesso in uso per scopi esclusivamente lavorativi. Al fine di controllo del corretto utilizzo dei servizi di fonia aziendale l'ente può esercitare i diritti di cui all'art. 124 D.Lgs. 196/2003 (fatturazione dettagliata) richiedendo ai provider di telefonia i dettagli necessari agli accertamenti sull'uso e relativo costo del traffico effettuato nel tempo.

I controlli saranno eseguiti secondo criteri e modalità descritte all'art. 5 del presente Regolamento. Qualora dall'esame del traffico di una singola utenza si rilevi uno scostamento significativo rispetto alla media del consumo sarà richiesto il tabulato analitico delle chiamate effettuate dalla SIM in incarico all'utente per il periodo interessato.

L'utilizzo dei dispositivi mobili risponde alle seguenti regole:

- Ciascun utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e conseguentemente, anche della sua diligente conservazione;
- In caso di furto, danneggiamento o smarrimento del dispositivo mobile l'utente assegnatario dovrà darne immediato avviso all'ente; se tali eventi siano riconducibili a un comportamento negligente o imprudente dell'utente stesso o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti;
- In caso di furto o smarrimento l'ente si riserva la facoltà di attuare la procedura di cancellazione da remoto di tutti i dati sul dispositivo, rendendo il dispositivo stesso inutilizzabile e i dati in esso contenuti del tutto irrecuperabili;
- Non è consentito all'utente caricare o inserire all'interno del dispositivo o SIM qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare o almeno ridurre la circolazione di dati personali sull'apparecchio, è obbligatorio cancellare tutti i dati eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione;
- Non è consentito all'utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi a meno che non siano strettamente connesse con il proprio compito lavorativo e siano

preventivamente autorizzate dall'ente;

- L'installazione di applicazioni, gratuite o a pagamento, su smartphone e tablet deve essere espressamente autorizzata, rimanendo in caso contrario a carico dell'utente le responsabilità derivanti dall'installazione non autorizzata che costituisce violazione del presente Regolamento;
- Salvo diversi specifici accordi derivanti da esigenze di servizio, al momento della consegna di tablet o smartphone l'utente è tenuto a verificare la disattivazione del sistema di geolocalizzazione potenzialmente attivabile sugli smartphone e tablet, consapevole che in caso contrario l'ente potrebbe venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e del suo assegnatario.

Capo IV — GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 14 – Gestione utilizzo della rete internet

Ciascun utente potrà essere abilitato alla navigazione Internet e pertanto si richiamano tutti gli utenti a una particolare attenzione al suo utilizzo consapevole così come dei servizi collegati, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato all'ente.

Ad ogni utente autorizzato è assegnata un account e una password per accedere alla rete wifi dell'Istituto. Per la gestione dell'account e della password assegnata si applicano le stesse disposizioni di cui agli art.7.1 e 7.2 del presente Regolamento.

L'accesso a internet attraverso i dispositivi dell'ente è autorizzato utilizzando esclusivamente la connessione dell'Istituto, dotata di opportuni firewall.

Solo nel caso di lavoro a distanza è consentito l'uso della rete privata per accedere, tramite le proprie password al server o alla piattaforma della scuola.

La connessione a Internet, in quanto strumento a disposizione degli utenti per uso professionale, deve essere utilizzata in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; ciò deve essere tenuto in considerazione in modo da prendere ogni precauzione conseguente.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

- L'utilizzo è consentito esclusivamente per scopi lavorativi e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
- Non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi espressamente autorizzati dall'ente;

- È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- Non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in guest-book, anche utilizzando pseudonimi (o nicknames);
- Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica;
- È consentito l'utilizzo di soluzioni di Instant Messanger o chat esclusivamente per scopi professionali e attraverso strumenti, software o piattaforme messi a disposizione dall'ente;
- Non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo;
- Non è consentito lo scambio o la condivisione di materiale audiovisivo, cinematografico, fotografico, informatico o altro anche se non protetto da copyright utilizzando sistemi Peer-to-Peer, a qualsiasi titolo e anche se non a scopo di lucro.
- Non è consentita la pubblicazione di immagini relative agli allievi se non con modalità che li rendano non identificabili. Ogni pubblicazione anche sul sito o sui profili social della scuola deve rispettare questo vincolo, salvo autorizzazione specifica rilasciata dai genitori, su richiesta esplicita dell'Istituto.Non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata preventivamente ed espressamente approvata.

È altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere in qualunque modo essere nocivo all'immagine dell'ente.

Per mezzo dell'Amministratore di Sistema e al fine di facilitare il rispetto delle predette regole l'ente ha configurato specifici filtri che inibiscono l'accesso ai contenuti non consentiti, con esclusione dei siti istituzionali, e che prevengono operazioni non correlate all'attività lavorativa.

Art. 15 – Gestione e utilizzo della posta elettronica aziendale

15.1 – Principi Guida

Per ciascun utente titolare di un account, l'ente provvede ad assegnare una casella di posta elettronica individuale.

I servizi di posta elettronica devono essere utilizzati a scopo professionale: l'account e-mail è uno strumento di proprietà dell'ente ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative affidate.

Ad uno stesso utente possono essere assegnate più caselle di posta elettronica, che possono anche essere condivise con altri utenti dello stesso gruppo/ufficio/dipartimento. Tali caselle di posta elettronica devono essere utilizzate esclusivamente per la ricezione dei messaggi mentre per le risposte o gli invii deve sempre essere utilizzata la casella personale.

Attraverso le caselle e-mail di istituto gli utenti rappresentano pubblicamente l'ente e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere positivamente l'immagine aziendale.

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica di Istituto conformemente alle presenti regole. Gli stessi devono:

- conservare la password nella massima riservatezza e con la massima diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
- utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (agenti di alterazione, ad esempio virus);
- inviare preferibilmente files in formato PDF;
- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i files attachment di posta elettronica prima del loro utilizzo;
- rispondere alle e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
- collegarsi a siti internet contenuti all'interno di messaggi solo per motivate ragioni e quando vi sia comprovata sicurezza sul contenuto degli stessi.

Inoltre, non è consentito agli utenti:

- diffondere il proprio indirizzo e-mail di Istituto attraverso la rete internet;
- utilizzare la casella di posta elettronica aziendale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, ecc., salvo che questo non sia funzionale all'attività prestata in favore dell'ente, per esempio presentazioni o materiali video ad uso didattico.

Salvo l'utilizzo di appositi strumenti di cifratura i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto si richiede agli utenti di valutare con attenzione l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale".

Occorre infine che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute da altri nell'organizzazione di appartenenza del mittente.

Per le comunicazioni verso l'ufficio di segreteria saranno accettate esclusivamente comunicazioni degli utenti provenienti dall'indirizzo di posta assegnato o dall'indirizzo del dominio @posta.istruzione.it. Essendo identificabile chiaramente il mittente, tali comunicazioni sono infatti considerate come sottoscritte ('firma debole') e pertanto assumibili agli atti della scuola.

15.2 – Cessazione dell'indirizzo di Posta Elettronica dell'Istituto

In caso di interruzione del rapporto di lavoro con l'utente, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 (trenta) giorni da quella data ed entro 90 (novanta) giorni si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, l'ente si riserva il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti per le proprie attività.

Capo V — GESTIONE DELLA DOCUMENTAZIONE CARTACEA

Art. 16 – Custodia della documentazione cartacea

La custodia dei documenti cartacei e analogici deve avvenire con modalità che garantiscano l'accesso alle sole persone autorizzate.

A tale scopo è necessario:

- NON lasciare mai incustoditi sulle scrivanie o in altro luogo i fascicoli, la corrispondenza o altri documenti che contengano dati personali o informazioni di carattere riservato;
- conservare i documenti contenenti dati personali o informazioni di carattere riservato in cartelline (non trasparenti), dossier e faldoni;
- non lasciare incustoditi documenti stampati su stampanti remote (nei corridoi, in altri locali, ecc.);
- i documenti contenenti dati personali o informazioni di carattere riservato di cui non è necessaria la conservazione devono essere distrutti in modo da renderne impossibile la lettura;
- archiviare gli eventuali dati appartenenti nel novero delle "particolari categorie di dati" ex articolo 9 Reg. UE 2016/679), secondo le modalità previste dal Manuale di Gestione del Flusso documentale dell'Istituto in modo che l'accesso sia selezionato, ovvero facendo sì che solo il personale autorizzato possa accedervi.
- conservare i documenti cartacei contenenti dati appartenenti nel novero delle

"particolari categorie di dati" ex articolo 9 Reg. UE 2016/679 in armadi o cassetti chiusi a chiave e prelevarli solo per il tempo necessario al trattamento

- non produrre copia di tali documenti, se non su autorizzazione scritta del Titolare del trattamento.

Art. 17 – Segnalazione accesso non autorizzato

Ogni accesso ai dati personali non consentito deve essere immediatamente segnalato al Titolare.

Capo VI - SANZIONI, COMUNICAZIONI, APPROVAZIONE

Art. 18 – Sanzioni

La violazione di quanto previsto dal presente Regolamento, rilevante anche ai sensi degli artt. 2104 e 2105 c.c., potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 (sanzioni disciplinari) della Legge 20 maggio 1970 n.300 (Statuto dei Lavoratori).

Nel caso venga commesso un reato o la cui commissione sia ritenuta probabile o solo sospettata l'ente avrà cura di informare senza ritardo, e senza necessità di preventive contestazioni o addebiti formali, le autorità competenti dell'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.

In caso di violazione accertata delle regole e degli obblighi esposti in questo Regolamento da parte degli utenti l'ente si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza o la funzionalità dei propri beni e strumenti informatici e inoltre per impedire il reitero di tale violazione.

Art. 19 – Informativa agli utenti ex art. 13 Regolamento (UE) 2016/679

Il presente Regolamento, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici aziendali e relativamente al trattamento di dati personali svolti dall'ente finalizzato all'effettuazione di controlli leciti, così come definiti nell'art. 5, vale quale informativa ex art. 13 del Regolamento (UE) 2016/679.

Art. 20 – Comunicazioni

Contestualmente all'assegnazione di un account il presente Regolamento è messo a disposizione degli utenti per la consultazione. La versione più aggiornata dello stesso è pubblicata sia in formato immateriale digitale che in formato fisico cartaceo allo scopo di facilitarne la diffusione a tutti gli interessati.

Per ogni aggiornamento del presente Regolamento sarà data comunicazione tramite apposita circolare a tutti gli utenti, che sono tenuti a conformarsi alla versione più aggiornata.

Le richieste di autorizzazione o concessione previste dal presente Regolamento

possono essere inoltrate all'ente per mezzo di qualsiasi strumento che ne garantisca la tracciabilità, ad esempio tramite e-mail, a cui è riconosciuto il valore di forma scritta in modo del tutto analogo rispetto a quella cartacea.

Art. 21 – Approvazione del Regolamento

Il presente Regolamento è stato approvato dal Legale Rappresentante dell'ente in data 14 novembre 2022, ed è stato oggetto di accordo con le rappresentanze sindacali aziendali in ottemperanza a quanto previsto dall'art. 4 della Legge 20 maggio 1970 n. 300 (Statuto dei Lavoratori).

REVELLO, 14 NOVEMBRE 2022

L'ente (nella persona del legale rappresentante)

LA DIRIGENTE SCOLASTICA
Paola MANIOTTI
Fto digitalmente ai sensi del D.lgs 82/2005