Regolamento per l'utilizzo degli strumenti informatici all'interno dell'Istituzione Scolastica (E-policy) – A.s. 2026/2027

Aggiornato al DPR n.81 del 13/06/2023 - Regolamento concernente modifiche al decreto del Presidente della Repubblica 16 aprile 2013, n. 62, recante: «Codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165».

Indice

Premessa

1. Entrata in vigore del Regolamento e pubblicità
2. Campo di applicazione del Regolamento
3. Utilizzo del Personal Computer
4. Gestione e assegnazione delle credenziali di autenticazione
5. Utilizzo della rete
6. Utilizzo di dispositivi elettronici
7. Utilizzo e conservazione dei supporti rimovibili
8. Utilizzo della posta elettronica
9. Navigazione in Internet e WiFi
10. Protezione antivirus
11. Partecipazione a social media
12. Osservanza delle disposizioni in materia di Privacy
13. Accesso ai dati trattati dall'utente
14. Regolamento BYOD
15. Altre disposizioni
16. Utilizzo del Registro elettronico e altre piattaforme digitali scolastiche
17. Sistema di controlli graduali
18. Aggiornamento e revisione

Premessa

La Scuola (di seguito "Titolare") ha disposto che al proprio interno venga osservato il presente Regolamento.
La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet da Personal Computer, tablet e smartphone, espone La Scuola e gli Utenti (dipendenti, collaboratori, studenti, chiunque acceda alla rete del titolare) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e disciplina sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine della Scuola stesso.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, La Scuola ha adottato un Regolamento interno diretto ad evitare che comportamenti anche inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati e quindi del proprio sistema informatico. Il Regolamento svolge anche la funzione di informare compiutamente gli utenti sugli specifici trattamenti dei loro dati personali che vengono effettuati, e delle modalità adottate.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite a tutti gli incaricati in attuazione del Regolamento Europeo sulla protezione dei dati (da ora in poi GDPR 2016/679), nonché integrano le informazioni già fornite agli interessati ai sensi dell'art. 13 del predetto regolamento, anche in ordine alle ragioni e alle modalità dei possibili controlli o alle conseguenze di tipo disciplinare in caso di violazione delle stesse.

Considerato inoltre che La Scuola, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, può mettere a disposizione dei propri utenti che ne necessitino per il tipo di funzioni svolte, telefoni, telefoni cellulari, computer portatili, tablet e smartphone, ecc., sono state inserite nel Regolamento alcune clausole relative alle modalità ed ai doveri che ciascun utente deve osservare nell'utilizzo di tale strumentazione.

Il presente Regolamento integra il Documento di indirizzo per la sicurezza informatica dell'Istituto ed è coerente con le Linee guida AgID e con il Piano Scuola 4.0.

Il Responsabile della Protezione dei Dati è contattabile all'indirizzo: rpd@progettoprivacy.it.

1. Entrata in vigore del Regolamento e pubblicità

1.1 Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate, qualora incompatibili o difformi, poiché sostituite dalle presenti.

1.2 Il presente Regolamento verrà portato a conoscenza anche di collaboratori, consulenti o altri incaricati esterni (es. incaricati software house, incaricati dei professionisti di cui si avvale La Scuola, etc.), studenti, famigliari che venissero autorizzati a far uso di strumenti tecnologici della Scuola o ad accedere alla rete informatica della scuola e ad eventuali dati ed informazioni ivi conservati e trattati. Pertanto, il presente regolamento entra a far parte, per quanto occorra, del Codice disciplinare della scuola.

2. Campo di applicazione del Regolamento

2.1 Il nuovo Regolamento si applica a tutti gli utenti, senza distinzione di ruolo e/o livello, nonché a tutti coloro che venissero autorizzati a far uso di strumenti tecnologici della Scuola o di accedere alla rete informatica della scuola e ad eventuali dati ed informazioni ivi conservati e trattati.

2.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve così intendersi ogni dipendente, collaboratore e/o consulente (come sopra già precisato), studente, famigliare autorizzato all'uso del sistema informatico.

3. Utilizzo del Personal Computer

3.1 Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività scolastica è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Il personal computer deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.

3.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete della Scuola solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto 4 del presente Regolamento.

3.3 La Scuola rende noto che il personale incaricato che opera presso il servizio di assistenza informatica (nel seguito per brevità "Servizio IT") della stessa è stato autorizzato a compiere interventi nel sistema informatico della scuola diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.). La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività della Scuola, si applica anche in caso di assenza prolungata o impedimento dell'utente. Qualora lo specifico intervento dovesse comportare anche l'accesso a contenuti delle singole postazioni PC, il servizio IT ne darà comunicazione agli utenti interessati, preventivamente ovvero, nel caso di urgenza dell'intervento stesso, successivamente ad esso.

3.4 Il personale incaricato del Servizio IT ha la facoltà di collegarsi e visualizzare in remoto i contenuti delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato su chiamata dell'utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

3.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale del Servizio IT per conto della Scuola né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone La Scuola a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate penalmente e possono anche comportare il sorgere di una responsabilità amministrativa a carico della Scuola, come disposta dall'art. 25-nonies del D.lgs. 8 giugno 2001, n. 231, con applicazione di sanzioni pecuniarie ed interdittive.

3.6 Salvo preventiva espressa autorizzazione del personale del Servizio IT, non è consentito all'utente modificare le impostazioni di sistema del proprio PC né procedere ad installare dispositivi hardware.

3.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale del Servizio IT nel caso in cui siano rilevati virus e adottando quanto previsto dal successivo punto 10 del presente Regolamento relativo alle procedure di protezione antivirus.

3.8 Il Personal Computer deve essere spento ogni sera prima di lasciare i locali della Scuola. In caso di suo inutilizzo, il pc deve essere bloccato e l'utente si deve scollegare dal pc: lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso.

4. Gestione e assegnazione delle credenziali di autenticazione

4.1 Le credenziali di autenticazione (utente e password) per l'accesso alla rete vengono assegnate dal personale del Servizio IT.

4.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio IT, associato ad una parola chiave (password) riservata che dovrà venir custodita dall'utente con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Servizio IT.

4.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri, di elevata complessità, non deve contenere riferimenti agevolmente riconducibili all'incaricato o all'user-id.

4.4 È necessario procedere alla modifica della parola chiave a cura dell'utente al primo utilizzo oppure in caso di perdita di qualità della stessa. Qualora venga scelta una parola chiave particolarmente complessa, può anche non essere modificata periodicamente.

4.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale del Servizio IT.

4.6 Si ricorda che, quando si utilizza un sistema condiviso con altri utenti, non si deve mai memorizzare alcuna password quali ad esempio quelle del registro elettronico o dell'account Google: memorizzando la password, altri utenti potrebbero facilmente accedere ai vostri dati personali.

4.7 È fatto espresso divieto di utilizzo dell'account Google della scuola quando si usa un pc non di proprietà della scuola o dell'intestatario.

5. Utilizzo della rete informatica

5.1 Per l'accesso alla rete della Scuola ciascun utente deve utilizzare esclusivamente la propria credenziale di autenticazione.

5.2 È assolutamente proibito entrare nella rete e nei programmi con una credenziale di autenticazione diversa da quello assegnata. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

5.3 Le cartelle utenti presenti nei server della Scuola sono aree di condivisione di informazioni e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività scolastica non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di manutenzione, amministrazione e back up da parte del personale del Servizio IT. Si ricorda che tutti i dischi o altre unità di memorizzazione locali - es. disco C: interno PC - non sono soggette a salvataggio da parte del personale incaricato del Servizio IT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

5.4 Il personale del Servizio IT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

5.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

5.6 In caso di utilizzo di pc condivisi, si raccomanda di non salvare files con dati personali in aree del pc a cui possono accedere altri utilizzatori.

5.7 Nella gestione dei sistemi informatici della scuola, il servizio IT potrà acquisire informazioni generate dalle funzionalità insite negli stessi sistemi, quali, ad esempio, le informazioni sugli orari di accensione e spegnimento dei personal computer, rilevati automaticamente tramite il sistema di autenticazione al dominio di rete, e i log degli accessi a specifiche risorse di rete (file o cartelle). Tali informazioni potranno essere utilizzate, ai sensi del successivo punto 12.2, per tutti i fini connessi al rapporto di lavoro, sempre nell'ambito delle finalità individuate nel precedente punto 3.3., e con espressa esclusione di qualsiasi forma di controllo sistematico e costante nei confronti degli utenti degli stessi sistemi.

5.8 Al termine del rapporto con l'utente, il servizio IT potrà riutilizzare il pc o dispositivo a lui rilasciato previa cancellazione di ogni file in esso contenuto (formattazione).

6. Utilizzo di altri dispositivi elettronici

6.1 Tutti i dispositivi elettronici dati in dotazione dalla Scuola devono considerarsi materiale scolastico: ne viene concesso l'uso esclusivamente per lo svolgimento delle attività scolastiche, non essendo quindi consentiti utilizzi a carattere personale o comunque non strettamente inerenti le attività scolastiche. Fra i dispositivi in questione vanno annoverati i telefoni della scuola, PC portatili, tablet, telefoni cellulari, smartphone, etc., indipendentemente dal fatto che l'utente abbia o meno la possibilità di accedere alla rete della Scuola o di condividere documenti, dati e materiali ivi conservati e/o trattati.

6.2 L'utente resta responsabile del singolo dispositivo assegnato e deve custodirlo con diligenza sia durante trasferte e spostamenti sia durante l'utilizzo nel luogo di lavoro; va sempre adottata ogni cautela per evitare danni o sottrazioni. In caso di smarrimento o furto di dispositivi le cui memorie possano essere cancellate o bloccate da remoto a cura del Servizio IT per evitare sottrazioni o diffusioni di dati incontrollati, l'utente dovrà immediatamente avvisare il servizio IT, e comunque al massimo entro 24 ore dal fatto.

6.3 Con riferimento ai telefoni della scuola e telefoni cellulari, fermo restando quanto sopra già disposto circa il loro uso e custodia, la ricezione o l'effettuazione di telefonate personali, così come l'invio o la ricezione di SMS o MMS di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività scolastica, viene consentita solo nel caso di comprovata necessità ed urgenza. Inoltre, l'eventuale uso promiscuo (anche per fini personali) del telefono cellulare della scuola è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal personale del Servizio IT.

6.4 Viene infine disposto il divieto di utilizzo per fini personali di strumenti della scuola, per spedire o per ricevere documentazione, e/o di fotocopiatrici della scuola, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio. **Tuttavia, al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere**

alle incombenze personali senza doversi allontanare dalla sede di servizio, purché' l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

7. Utilizzo e conservazione dei supporti rimovibili

7.1 Tutti i supporti magnetici rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how della scuola, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

7.2 L'utente resta, in ogni caso responsabile della custodia dei supporti e dei dati della scuola in essi contenuti; in particolare, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

7.3 Qualora non disposto diversamente, si sconsiglia l'utilizzo di supporti rimovibili personali (chiavette Usb).

7.4 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il personale del Servizio IT e seguire le istruzioni da questo impartite. Nel caso di dispositivi elettronici, con riferimento in particolare a PC portatili, tablet ed altri dispositivi sui quali possano venir salvati documenti, dati ed altro materiale, dovrà farsi particolare attenzione al salvataggio in opportuni supporti esterni di tale materiale oppure alla sua rimozione effettiva prima della riconsegna del dispositivo, concordata comunque ogni opportuna azione al riguardo con il personale del Servizio IT.

7.5 In caso di smarrimento di una chiavetta USB contenente dati personali, avvisare immediatamente il Dirigente scolastico e il Responsabile della protezione dei dati (rpd@progettoprivacy.it).

8. Utilizzo della posta elettronica

8.1 La casella di posta elettronica assegnata all'utente è uno strumento da utilizzarsi solo per le attività scolastiche**.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

8.2 È fatto divieto di utilizzare le caselle di posta elettronica della scuola per motivi diversi da quelli strettamente legati all'attività scolastica. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es. mp3) non legati all'attività scolastica;
- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o c.d. "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, lo si dovrebbe comunicare immediatamente al personale del Servizio IT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

8.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili o non costituenti corrispondenza scolastica e soprattutto allegati ingombranti. In caso di cessazione del rapporto con La Scuola, quest'ultima provvederà, con congruo preavviso e trasferimento dei documenti istituzionali, alla sospensione e successiva eliminazione dell'account di posta e dei relativi messaggi ivi contenuti.

8.4 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

8.5 È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web non conosciuti).

8.6 Al fine di garantire la funzionalità del servizio di posta elettronica della scuola e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività fuori sede dell'assegnatario della casella) potrà inviare automaticamente messaggi di risposta contenenti le coordinate di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata e disattivata dall'utente.

8.7 Le presenti regole si applicano anche nel caso in cui venisse assegnato all'utente anche la gestione di uno o più indirizzi di posta elettronica certificata.

8.8 L'indirizzo e-mail è un dato personale e non va rivelato ad alcuno se non necessario: in caso di invio di circolari per e-mail non si devono quindi mettere gli indirizzi e-mail dei destinatari in chiaro nel campo CC ma invece nel campo CCN in modo che non siano visibili agli altri.

8.9 L'indirizzo e-mail viene cancellato alla cessazione del rapporto con la scuola e tutti i dati contenuti vengono di conseguenza eliminati.

8.10 L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può' in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione. L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale. Il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'amministrazione di appartenenza. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.

8.11 E' vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.

9. Navigazione in Internet e WiFi

Le seguenti disposizioni sono valide sia per chi utilizza strumenti scolastici che strumenti personali.

9.1. Durante l'utilizzo di internet all'interno della scuola è assolutamente proibita la navigazione per motivi diversi da quelli strettamente legati all'attività scolastica.

9.2 In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:
- l'upload o il download di software anche gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività scolastica e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venir a tal fine contattato il personale del Servizio IT);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Dirigenza (o eventualmente dal Responsabile d'ufficio e/o del Servizio IT) e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività scolastica;
- l'iscrizione con account della scuola e la partecipazione personale a social network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames);
- collegamenti a servizi P2P (torrent, e-mule, file sharing) o lo scaricamento di contenuti multimediali per finalità ludiche. Sono altresì vietati collegamenti a siti di gioco online.

9.3 Al fine di evitare la navigazione in siti non pertinenti all'attività scolastica, La Scuola rende peraltro nota la possibile adozione di uno specifico sistema di blocco o filtro automatico che prevenga determinate operazioni quali l'upload o l'accesso a determinati siti.

9.4 Si informano gli utenti che, in caso di malfunzionamenti, blocchi, segnalazioni di disservizio sulla rete internet, il Servizio IT può effettuare, con la sola finalità di individuare il problema, dei controlli sui file di log contenenti le tracce di navigazione degli utenti. I file di log vengono conservati per un periodo di tempo massimo di sei mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza della Scuola.

9.5 L'utilizzo di tutte le reti WiFi presenti presso La Scuola è limitato agli utenti autorizzati. A tale scopo si precisa che l'utilizzo di qualsiasi rete WiFi disponibile è possibile solo a seguito di digitazione di specifiche credenziali che vengono assegnate dal reparto IT o tramite la digitazione di una password di accesso. È assolutamente vietato comunicare a terzi non autorizzati e non facenti parte della comunità scolastica la password o le credenziali di accesso alle reti WiFi scolastiche.

9.6 Non è consentito l'accesso a siti e servizi che prevedano un traffico di dati sulla rete tali da pregiudicare il buon funzionamento della medesima.

9.7 Durante l'utilizzo della rete Internet è vietato:
- svolgere qualunque attività che sia in contrasto con la normativa italiana ed europea;
- accedere a siti che per contenuti ed immagini siano in contrasto con le finalità servizio e/o illegali (siti pedofili, pornografici, che ispirano alla violenza, al razzismo, ecc.);
- inviare messaggi di posta secondo modalità indiscriminate (spamming);
- svolgere qualsiasi attività intesa ad eludere o ingannare i sistemi di controllo di accesso e/o sicurezza di qualsiasi server interno esterno pubblico o privato
- usare meccanismi o strumenti di qualsiasi natura atti ad eludere i sistemi di protezione da copia abusiva del software, a rivelare password, ad identificare eventuali vulnerabilità della sicurezza dei vari sistemi, a decriptare file crittografati o a compromettere la sicurezza della rete in qualsiasi modo

9.10 L'utente è direttamente responsabile delle attività svolte durante la connessione a Internet: le conseguenze penali e civili derivanti da un uso fraudolento della medesima rete e ogni responsabilità civile e penale è in capo ai singoli utilizzatori della rete Internet.

10. Protezione antivirus

10.1 Il sistema informatico della Scuola è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico della scuola mediante virus o mediante ogni altro software aggressivo.

10.2 Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale del Servizio IT.

10.3 Ogni dispositivo magnetico di provenienza esterna dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale del Servizio IT.

11. Partecipazioni a social media

11.1 L'utilizzo dei social media ufficiali della Scuola – quali Facebook™, Twitter™, Linkedin™, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dalla Dirigenza attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti.

11.2 Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, La Scuola ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio della scuola, anche immateriale, quanto i propri collaboratori e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione dal Titolare, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali.

11.3 La condivisione dei contenuti nei social media deve sempre rispettare e garantire i diritti dei soggetti coinvolti. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che della Scuola.

11.4 L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori della scuola e di studenti, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi della scuola, se non con il preventivo consenso della Dirigenza.

11.5 L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso la Scuola, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano

molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito della scuola.

11.6 Nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla pubblica amministrazione di appartenenza. In ogni caso, il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.

11.7 Le amministrazioni si possono dotare di una "social media policy" per ciascuna tipologia di piattaforma digitale, al fine di adeguare alle proprie specificità le disposizioni di cui al presente articolo. In particolare, la "social media policy" deve individuare, graduandole in base al livello gerarchico e di responsabilità del dipendente, le condotte che possono danneggiare la reputazione delle amministrazioni.

11.8 Fermi restando i casi di divieto previsti dalla legge, i dipendenti non possono divulgare o diffondere per ragioni estranee alloro rapporto di lavoro con l'amministrazione e in difformità alle disposizioni di cui al decreto legislativo 13 marzo 2013, n. 33, e alla legge 7 agosto 1990, n. 241, documenti, anche istruttori, e informazioni di cui essi abbiano la disponibilità attribuibili direttamente alla pubblica amministrazione di appartenenza.

11.9 In ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine dell'amministrazione di appartenenza o della pubblica amministrazione in generale.

11.10 Al fine di garantirne i necessari profili di riservatezza le comunicazioni, afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche

11.11 L'Istituto si riserva di adottare una specifica Social Media Policy, in conformità al D.P.R. 62/2013 e alle linee guida AgID, che regoli nel dettaglio l'utilizzo dei canali social ufficiali e l'eventuale partecipazione del personale.

12. **Osservanza delle disposizioni in materia di Privacy**

12.1 È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure adeguate di sicurezza dei dati personali.

12.2 In caso di rapporto di lavoro, gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo e terzo, della Legge n.300/1970; conseguentemente, le informazioni raccolte sulla base di quanto indicato nel Regolamento, anche conformemente al successivo punto 13, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico della scuola ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero venir eventualmente compiuti, fermo restando il rispetto della normativa in materia di protezione dei dati personali (GDPR 2016/679).

12.3 Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori e di altri soggetti che utilizzano la rete scolastica; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio della scuola, La Scuola provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970, dandone anche opportuna informazione agli utenti stessi.

13. Accesso ai dati trattati dall'utente

13.1 Oltre che per motivi di sicurezza del sistema informatico, compresi i motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.), per finalità di controllo e programmazione dei costi della scuola (ad esempio, verifica costi di connessione a Internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività degli utenti, è facoltà della Direzione della scuola, tramite il personale del Servizio IT o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy e delle procedure, agli strumenti informatici della scuola e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

13.2 In caso di anomalie, il personale incaricato del servizio IT effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti agli utenti dell'area o del settore in cui è stata rilevata l'anomalia (classe, ufficio), nei quali si evidenzierà l'utilizzo irregolare degli strumenti della scuola e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base più ristretta o anche individuale potranno essere computi solo in caso di successive ulteriori anomalie.
Si avvisa che nei computer scolastici potrà essere installato un software di controllo remoto al fine di agevolare le operazioni di manutenzione e assistenza tecnica.
L'amministrazione, attraverso i propri responsabili di struttura, ha facoltà di svolgere gli accertamenti necessari e adottare ogni misura atta a garantire la sicurezza e la protezione dei sistemi informatici, delle informazioni e dei dati. Le modalità di svolgimento di tali accertamenti sono stabilite mediante linee guida adottate dall'Agenzia per l'Italia Digitale, sentito il Garante perla protezione dei dati personali. In caso di uso di dispositivi elettronici personali, trova applicazione l'articolo 12, comma 3-bisdel decreto legislativo 7 marzo 2005, n. 82.

I controlli individuali, ove necessari, saranno effettuati nel rispetto dei principi di finalità, necessità e proporzionalità di cui all'art. 5 del GDPR, previa registrazione scritta della motivazione e nel rispetto della riservatezza

14. Regolamento BYOD

Il termine "Bring your own device" (BYOD) - in italiano: "porta il tuo dispositivo" - è un'espressione usata per riferirsi alle politiche che permettono di portare i propri dispositivi personali a scuola e di usarli per avere gli accessi veloci alle informazioni scolastiche e alle loro applicazioni.
La Scuola del trattamento autorizza l'utilizzo in ambito scolastico l'uso dei dispositivi di proprietà degli utenti, all'interno dei quali verranno quindi memorizzati dati e informazioni relative alle attività scolastiche, contenenti anche dati personali. Un tipico utilizzo è l'accesso alla posta elettronica e Drive scolastici dallo smartphone/tablet di proprietà personale. Per essere autorizzato, tale utilizzo è vincolato alle seguenti norme di utilizzo che andranno scrupolosamente osservate:

1. È obbligatorio dotare il proprio dispositivo di un dispositivo di protezione (PIN, impronta, ecc) ad esclusiva conoscenza del soggetto autorizzato (e non dei suoi famigliari/amici)
2. Qualora non si volesse bloccare il dispositivo con pin di protezione, è obbligatorio dotare di password l'accesso alle funzionalità di posta elettronica o ai drive condivisi del titolare. Tale password non va mai memorizzata e deve sempre essere richiesta per accedere ai dati di proprietà del titolare.
3. Nella vita privata, le funzioni e i dati personali devono essere protetti da accessi da parte di terzi (famigliari, amici, ecc)
4. Qualora il dispositivo venisse ceduto o dato in uso, anche temporaneo, ad altri soggetti, il soggetto autorizzato è tenuto a cancellare ed eliminare tutti gli accessi alla posta elettronica e ai dati personali. Il soggetto autorizzato sarà considerato responsabile civilmente e penalmente di quanto attribuito al proprio codice di accesso personale (user-id).
5. È vietato salvare localmente in modo permanente dati sensibili o riservati, appartenenti a categorie particolari di dati personali.
6. In caso di smarrimento o accesso non autorizzato, è obbligatorio segnalare l'accaduto al RPD e al Dirigente Scolastico entro 24 ore.

15. Altre disposizioni

15.1 È vietato salvare sul personal computer e sul server della scuola per scopi personali files contenenti dati ritenuti sensibili, quali ad esempio copie delle buste paga (dipendenti) o altri dati sensibili quali esami, visite mediche, ecc. in qualsiasi formato.

15.2 La riservatezza dei dati personali è un valore per La Scuola ed occorre quindi che tutti gli attori, interni ed esterni, siano consapevoli che è vietato comunicare ad estranei contatti e altri dati patrimonio della scuola.

16. Utilizzo del Registro elettronico e altre piattaforme digitali scolastiche

16.1 L'utente è tenuto a osservare le specifiche disposizioni relative all'utilizzo del registro elettronico e delle piattaforme didattiche digitali a cui ha ottenuto accesso (Google Workspace for education, Microsoft for Education, Weschool, ecc.)

17. Utilizzo di sistemi di intelligenza artificiale

17.1 L'utilizzo, nell'ambito delle attività didattiche, amministrative e organizzative dell'Istituto, di sistemi e servizi basati sull'intelligenza artificiale è consentito esclusivamente mediante strumenti preventivamente valutati e autorizzati dalla Scuola. Non è consentito utilizzare account istituzionali per accedere a servizi di IA non autorizzati né comunicare a tali servizi dati personali, documenti riservati o informazioni dell'Istituto.

17.2 Gli utenti devono rispettare i principi di necessità, minimizzazione, riservatezza, sicurezza, trasparenza e controllo umano. Nei sistemi di IA non devono essere inseriti dati appartenenti a categorie particolari, dati giudiziari, informazioni relative a disabilità, salute, situazioni familiari, procedimenti disciplinari o altri dati riservati, salvo che il trattamento sia stato specificamente autorizzato dall'Istituto e accompagnato dalle necessarie garanzie.

17.3 I risultati prodotti dai sistemi di IA devono essere sottoposti a verifica critica da parte dell'utilizzatore. Gli strumenti di IA non possono sostituire la responsabilità professionale del personale scolastico né assumere autonomamente decisioni riguardanti valutazione, ammissione, orientamento, assegnazione di attività, provvedimenti disciplinari o altri aspetti significativi relativi agli studenti o al personale.

17.4 L'utilizzo dei sistemi di IA avviene nel rispetto del Regolamento d'Istituto per l'utilizzo dell'intelligenza artificiale, della Policy per l'uso dell'IA, delle informative sul trattamento dei dati personali, dell'eventuale Registro degli strumenti IA e delle specifiche istruzioni operative adottate dalla Scuola. Quando il trattamento è facoltativo o coinvolge studenti minorenni, sono acquisite le autorizzazioni o i consensi previsti dalla normativa e sono assicurate modalità alternative adeguate.

17.5 Prima dell'introduzione di un nuovo sistema, l'Istituto ne valuta le finalità, i dati trattati, il ruolo del fornitore, le condizioni contrattuali, i limiti di età, i trasferimenti verso Paesi terzi, l'eventuale utilizzo dei dati per l'addestramento dei modelli e i rischi per i diritti e le libertà degli interessati. Quando ricorrono i presupposti dell'art. 35 del GDPR, è effettuata una valutazione d'impatto sulla protezione dei dati.

17.6 Il personale e gli studenti utilizzano gli strumenti di IA secondo il proprio ruolo, il livello di autorizzazione ricevuto e le istruzioni impartite dall'Istituto. Le violazioni delle presenti disposizioni possono comportare la sospensione dell'accesso al servizio e l'applicazione delle misure previste dai regolamenti scolastici e dalla normativa vigente.

Per ulteriori informazioni si vedano:
- Regolamento per l'utilizzo dei sistemi di IA, contenente principi, ruoli, usi consentiti e vietati;
- Policy per l'uso dell'intelligenza artificiale – PUIA, con istruzioni operative per personale e studenti;
- Informativa privacy IA, da utilizzare solo per trattamenti concretamente individuati;
- Registro o elenco degli strumenti IA autorizzati, preferibilmente interno, con una parte informativa accessibile a studenti e famiglie;

18. Aggiornamento e revisione

18.1 Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Dirigenza scolastica.

18.2 Il presente Regolamento è soggetto periodicamente a revisione.

Il Dirigente Scolastico