



I.C. C. SALUTATI



A. CAVALCANTI

P.zza A. Moro, 1 51011 Buggiano (PT) Centralino: (+39) 0572 32018

Email: ptic81900g@istruzione.it PEC: ptic81900g@pec.istruzione.it

Codice fiscale: 81003470473 Codice meccanografico: PTIC81900G

Codice Indice delle Pubbliche Amministrazioni (IPA): ISTSC_81900G



REGOLAMENTO SULL'UTILIZZO DELLA STRUMENTAZIONE DIGITALE E RETE INTERNET

IL CONSIGLIO DI ISTITUTO

➤ VISTO il regolamento di istituto, di cui questo regolamento è parte integrante

ADOTTA

il seguente regolamento sull'utilizzo della strumentazione digitale e rete internet
con Delibera n. 10 a. s. 2025-26 dell'11/02/2026

CAPO I – I PRINCIPI

Articolo 1 - Termini e definizioni

1. All'interno del presente regolamento e nell'Istituto si adottano i seguenti termini e le seguenti definizioni:
 - a. **chat**: servizio offerto da Internet, che mediante apposito software permette a più interlocutori di conversare scambiandosi messaggi scritti che appaiono in tempo reale sul monitor di ciascuno;
 - b. **client**: personal computer collegato in rete a un altro computer (server), sul quale risiedono i dati che il primo utilizza;
 - c. **computer portatile**: elaboratore elettronico istituzionale trasportabile con facilità;
 - d. **e-mail**: messaggio inviato tramite posta elettronica;

- e. **titolare**: L'I.C. Salutati – Cavalcanti rappresentato legalmente dal dirigente scolastico;
- f. **estensione**: set di tre lettere che segue il nome di un file di un computer e ne identifica il genere;
- g. **log**: registrazione ufficiale di eventi;
- h. **password**: parola o sigla di riconoscimento fornita dall'utente al computer per poter accedere a un sistema operativo a un programma o a un file;
- i. **peer to peer**: sistema di computer collegati gli uni agli altri senza la connessione ad un server;
- j. **personal computer**: elaboratore elettronico destinato all'uso istituzionale;
- k. **phishing**: l'attività criminale di mandare e-mail o costituire un sito web al fine; di ingannare qualcuno e carpire informazioni (es. numeri di carta di credito o password);
- l. **rete Istituzionale**: sistema di trasmissione delle informazioni costituito da linee di collegamento e da stazioni che possono essere costituite da elaboratori, terminali o unità di memoria;
- m. **servizi ICT**: (Information and Communication Technologies) Tecnologie riguardanti i sistemi integrati di telecomunicazione (linee di comunicazione cablate e senza fili), i computer, le tecnologie audio-video e relativi software, che permettono agli Utenti di creare, immagazzinare e scambiare informazioni;
- n. **piattaforma informatica di istituto**: qualsiasi piattaforma gestita dall'istituto e il cui accesso è fornito dallo stesso;
- o. **e-mail di servizio**: e-mail fornita dall'Istituto e ad estensione @istitutosalutaticavalcanti.it;

- p. **server**: computer collegato in rete ad altri computer (client), sul quale risiedono i dati che questi utilizzano;
- q. **smartphone**: apparecchio elettronico che combina le funzioni di un telefono cellulare e di un computer palmare.
- r. **spamming**: mandare messaggi a diverse persone tramite e-mail o internet generalmente a fini commerciali;
- s. **tablet**: elaboratore elettronico istituzionale compatto con interfaccia touch;
- t. **dispositivi di memoria portatili**: tutti quei dispositivi che consentono di copiare o archiviare dati, file o documenti esternamente al computer. Sono considerati tali CD-ROM, DVD, penne o chiavi di memoria USB, fotocamere digitali, dischi rigidi esterni, ecc.;
- u. **utente**: coloro che si servono di un'attrezzatura o servizi ICT forniti dall'Istituto e che di seguito sono individuati:
 - i. personale della scuola (tempo indeterminato e determinato) fino al termine dell'attività lavorativa presso l'Istituto;
 - ii. famiglie degli studenti/alunni/bambini dell'Istituto;
 - iii. altre categorie di Utenti che possono richiedere la creazione di un account, come ospiti;
 - iv. consiglieri del Consiglio di Istituto della componente genitori;

Articolo 2 - Scopo

1. L'istituto utilizza le piattaforme informatiche e i servizi I.T.C. per:
 - a. gestire gli aspetti burocratici nell'ambito delle proprie finalità;
 - b. a supporto dell'ampliamento dell'offerta formativa dell'Istituto;
 - c. come supporto alla didattica innovativa e per lo sviluppo delle competenze digitali;
 - d. come supporto al diritto all'istruzione nei casi in cui non sia possibile

garantire la presenza scolastica;

e. per potenziare le relazioni e la comunicazione Scuola-Famiglia;

f. per potenziare la comunicazione tra il personale docente finalizzata alla condivisione e al lavoro di gruppo.

2. Lo scopo del presente Regolamento è di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione informatica da parte degli Utenti assegnatari (personale, studenti, collaboratori esterni, famiglie etc.), al fine di tutelare i beni istituzionali ed evitare condotte inconsapevoli e/o scorrette che potrebbero esporre l'Istituto a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.

L'insieme delle norme comportamentali ivi incluse, pertanto, è volto a conformare il Titolare ai principi di diligenza, informazione e correttezza nell'ambito dei rapporti di lavoro e istituzionali, con l'ulteriore finalità di prevenire eventuali comportamenti illeciti dei dipendenti e degli Utenti in generale, pur nel rispetto dei diritti ad essi attribuiti dall'ordinamento giuridico italiano. A tal fine, pertanto, si rileva che gli eventuali controlli ivi previsti escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento (UE) n. 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 – di seguito anche solo GDPR)), alla Legge n. 300/1970 (c.d. Statuto dei Lavoratori) alla luce delle modifiche intervenute ad opera del D.lgs. 14 settembre 2015, n. 151 ed ai provvedimenti appositamente emanati dall'Autorità Garante (si veda in particolare provv. 1° marzo 2007 oggi vigente).

Articolo 3 - Applicabilità

1. La presente procedura si applica a tutto il personale dell'Istituto, nonché al personale esterno e alle famiglie assegnatarie di beni e risorse informatiche istituzionali ovvero utilizzatrici di servizi e risorse informative di pertinenza del Titolare.

Articolo 4 - Titorarietà dei beni e delle risorse informatiche

1. I beni e le risorse informatiche, i servizi ICT e le reti informatiche costituiscono beni istituzionali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà del Titolare.
2. Il loro utilizzo, pertanto, è consentito solo per finalità di adempimento delle mansioni lavorative o istituzionali affidate ad ogni Utente in base al rapporto in essere per l'esclusivo perseguimento degli obiettivi istituzionali. A tal fine si precisa sin d'ora che qualsivoglia dato e/o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà del Titolare, sarà dalla stessa considerata come avente natura istituzionale e non riservata.

Articolo 5 - Responsabilità personale dell'utente

1. Ogni Utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche affidatigli dal Titolare nonché dei relativi dati trattati per finalità istituzionali.
2. A tal fine ogni Utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con il Titolare, è tenuto a tutelare (per quanto di propria competenza) il patrimonio istituzionale da utilizzi impropri e non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse istituzionali. Ogni Utente, pertanto, è tenuto, in relazione al proprio ruolo e alle mansioni in concreto svolte, ad operare a

tutela della sicurezza informatica istituzionale, riportando al proprio responsabile e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente Regolamento.

3. Sono vietati comportamenti che possano creare un danno, anche di immagine, al Titolare.

CAPO II – MISURE ORGANIZZATIVE

Articolo 6 - Amministratori del sistema

1. Il Titolare conferisce all'amministratore di sistema il compito di sovrintendere i beni e le risorse informatiche istituzionali. I principali compiti, a titolo meramente esemplificativo e non esaustivo sono:
 - a. gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza del Titolare;
 - b. 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;
 - c. 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;
 - d. 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;
 - e. rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli Utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
 - f. provvedere alla sicurezza informatica dei sistemi informativi

istituzionali, nel rispetto di quanto prescritto dal G.D.P.R.;

g. 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 ad un Utente in caso di prolungata assenza, irreperibilità o impedimento dello stesso. Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di Responsabile Privacy all'interno del Titolare e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.

2. L'Amministratore di sistema è individuato dal dirigente scolastico. Se non sono presenti all'interno dell'Istituto figure qualificate nomina un consulente esterno; in questo caso l'amministratore di sistema è coadiuvato dall'Animatore digitale.

Articolo 7 - Assegnazione degli account e gestione delle password

Creazione e gestione degli Account Utente

1. Gli account Utente sono creati per:

a. il personale della scuola (tempo indeterminato e determinato) fino al termine dell'attività lavorativa presso l'Istituto.

b. le famiglie degli studenti/alunni/bambini dell'Istituto, previa compilazione e consegna del modulo di consenso firmato;

c. altre categorie di Utenti che possono richiedere la creazione di un account, come ospiti; in questo caso l'accoglimento della domanda è a discrezione del dirigente scolastico;

d. i consiglieri del Consiglio di Istituto della componente genitori;

2. Un account Utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche istituzionali,

per singola postazione lavorativa. La gestione di tali account segue quanto sotto espressamente previsto:

- a. l'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione" (es. "Username" e "Password"), comunicate all'Utente dall'amministratore di sistema, che le genera, attraverso modalità che ne garantiscano la segretezza;
- b. le credenziali di autenticazioni costituiscono dati istituzionali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi;
- c. 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, lo stesso è tenuto a modificare immediatamente la password e/o a segnalare la violazione all'amministratore del sistema nonché al Responsabile privacy di riferimento;
- d. ogni Utente è responsabile dell'utilizzo del proprio account Utente;
- e. in caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per le esigenze produttive istituzionali o per la sicurezza ed operatività delle risorse informatiche del Titolare, la stessa si riserva la facoltà di accedere a qualsiasi dotazione e/o apparato assegnato in uso all'Utente per mezzo dell'intervento dell'Amministratore di sistema.
- f. Le famiglie sono responsabili della conservazione dei codici identificativi dei propri figli che per motivi di privacy sono forniti dall'Istituto.

Gestione e utilizzo delle password

3. Dopo la prima comunicazione delle credenziali di autenticazione da

parte dell'amministratore di sistema, l'Utente ha il compito di modificare, al suo primo utilizzo, la propria password, procedendo allo stesso modo ogni 12 mesi.

4. L'Utente, nel definire il valore della password, deve rispettare le seguenti regole:

- a. utilizzare almeno 8 caratteri alfanumerici, inclusi i caratteri speciali (#, %, etc.);
- b. utilizzare almeno tre delle seguenti categorie: un carattere maiuscolo, un carattere minuscolo, un numero, un carattere non alfanumerico tipo "@, £, \$, €, &#, \$";
- c. evitare di includere parti del nome, cognome e/o comunque elementi a lui agevolmente riconducibili;
- d. evitare l'utilizzo di password comuni e/o prevedibili;
- e. evitare di scegliere password che si possono trovare in un dizionario, anche di lingua straniera;
- f. evitare di salvare automaticamente la password per successivi utilizzi delle applicazioni;
- g. evitare di scrivere la password in posti in cui possa essere letta (ad es. vicino al computer);
- h. quando viene immessa la password accertarsi di non essere osservati.
- i. proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi.

5. Nel caso in cui l'utente acceda a banche dati dove, per limitazioni tecnologiche, non sia possibile impostare la scadenza automatica della password, sarà obbligo e cura dell'utente gestire la propria password nelle modalità sopra indicate.

6. Scrivere la password su post-it o altri supporti (ivi compresa la sua memorizzazione sul telefono/smartphone istituzionale) non è conforme alla normativa e costituisce violazione del presente Regolamento.

Cessazione degli Account

7. In caso di interruzione del rapporto di lavoro o di termine del percorso scolastico con l'Utente, le credenziali di autenticazione di cui sopra verranno disabilitate entro un periodo massimo di 2 giorni da quella data.
8. Qualora vi sia richiesta di reset password di un utente a qualsiasi titolo, perché, per esempio, sussiste il dubbio che terzi ne siano venuti a conoscenza o perché dimenticata, l'amministratore di sistema procederà a riassegnare una nuova password temporanea al fine di consentire all'utente l'accesso ai sistemi presso cui è accreditato, con l'impegno di modificarla subito dopo nei termini sopra individuati.

Articolo 8 - Postazioni di lavoro

1. Per postazione di lavoro si intende il complesso unitario di Personal Computer (di seguito, PC), notebook, accessori, periferiche e ogni altro *device* concesso dal Titolare in utilizzo all'Utente. L'assegnatario di tali beni e strumenti informatici istituzionali, pertanto, ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile.
2. Al fine di disciplinare un corretto utilizzo di tali beni, il Titolare ha adottato le regole tecniche, che di seguito si riportano:
 - a. la postazione di lavoro, sia essa acquistata, noleggiata, o affidata in comodato d'uso gratuito, rimane di esclusiva proprietà del Titolare, ed è concesso all'Utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti all'attività svolta;

- b. è dovere di ogni Utente usare la postazione di lavoro a lui affidati responsabilmente e professionalmente;
- c. la postazione di lavoro di cui sopra deve essere utilizzata con hardware e software autorizzati dal Titolare. Per utilizzare software o applicativi non presenti nella dotazione standard fornita, è necessaria una espressa autorizzazione del Titolare;
- d. la postazione di lavoro non deve essere lasciata incustodita con le sessioni Utenti attive;
- e. quando un Utente si allontana dalla propria postazione di lavoro, deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione;
- f. ogni dispositivo di proprietà dell'Istituto deve possedere una password di accesso scelta dalla D.S.G.A. per gli uffici amministrativi e dall'animatore digitale per i dispositivi didattici; le password sono condivise esclusivamente con gli Utenti autorizzati di seguito descritti ed è fatto divieto di modificarle. La conservazione e la modifica di qualunque password è diretta responsabilità della D.S.G.A. e dell'animatore digitale ognuno secondo i propri compiti;
- g. in assenza della D.S.G.A. la modifica è fatta dal dirigente scolastico, titolare del trattamento dati;
- h. tutti i dispositivi elettronici dell'Istituto devono essere catalogati dall'animatore digitale con una sigla che deve possedere le seguenti caratteristiche: ICSCXXX dove XXX è un numero progressivo da 001;
- i. l'Utente deve segnalare con la massima tempestività all'amministratore del sistema ovvero al proprio Responsabile di riferimento eventuali guasti tecnici, problematiche tecniche o il

- cattivo funzionamento della postazione di lavoro;
- j. è fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici istituzionali a soggetti terzi;
3. il Titolare si riserva la facoltà di rimuovere qualsiasi elemento hardware la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata.
4. Gli apparecchi di proprietà personale dell'Utente quali computer portatili, telefoni cellulari, agende palmari (PDA), hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali, ecc. non potranno essere collegati ai computer o alle reti informatiche istituzionali, salvo preventiva autorizzazione del responsabile; infine, si precisa che tutti i file di provenienza incerta, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo ed alla relativa autorizzazione del Servizio ICT.
5. Non potendo l'Istituto fornire un dispositivo elettronico di lavoro ad ogni singolo dipendente, non è possibile porre il divieto all'Utente di collegarsi, anche attraverso servizi *webmail*, agli account istituzionali (Argo Didup, piattaforma di istituto, ecc.) mediante telefono cellulare/smartphone personali. In questo caso il dipendente è comunque tenuto al rispetto delle regole tecniche imposte al comma 2 lettere: b) c) d) e) ed i); è consigliato seguire la regola tecnica di cui al comma 2 lettera j). Considerato che il personale di questo istituto è stato autorizzato al trattamento dati secondo il proprio ruolo, ha una responsabilità personale (*accountability*) della protezione della privacy altrui; pertanto, si dispone l'obbligo di immediata comunicazione all'Amministrazione, nella persona del Titolare, in caso di eventuali furti o smarrimenti dei dispositivi non di proprietà dell'Istituto, ma ricollegabili alle attività lavorative, al fine di limitare gli effetti

di data breach.

CAPO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Articolo 9 - Personal computer, computer portatili

1. Il personal computer, il computer portatile presente sul proprio posto di lavoro o assegnato sono considerati quali strumenti di lavoro di proprietà del Titolare, e devono essere utilizzati per compiere mansioni lavorative. Ne consegue che gli Utenti sono tenuti al rispetto delle seguenti regole:
 - a. non è consentito modificare la configurazione hardware e software del proprio PC, se non previa esplicita autorizzazione del Titolare;
 - b. non è consentito rimuovere, danneggiare o asportare componenti hardware;
 - c. non è consentito installare autonomamente programmi informatici, software ed ogni altro applicativo non autorizzato espressamente dal Titolare;
 - d. non è consentito connettere al personal computer, al computer portatile, o alla rete istituzionale apparecchi elettronici (telefoni cellulari personali o istituzionali, agende elettroniche, PC portatili, chiavi USB, ecc.);
 - e. è onere dell'Utente, in relazione alle sue competenze, 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 sistema;
 - f. è onere dell'Utente spegnere tutti i dispositivi elettronici della propria postazione di lavoro al termine della giornata lavorativa.
2. Per quanto concerne, invece, la gestione dei computer portatili, l'Utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli

spostamenti, rimuovendo gli eventuali *file* elaborati prima della sua riconsegna.

3. Non è consentito all'Utente caricare o inserire all'interno del portatile qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda agli Utenti di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile agli uffici competenti per la restituzione o la riparazione. Nel caso in cui l'Utente vi conservi, contrariamente alle direttive impartitegli, dati di natura personale, il Titolare in nessun caso potrà essere ritenuto responsabile della salvaguardia o della perdita di tali dati.
4. L'amministratore di sistema ha la facoltà di controllare le singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc.

Articolo 10 - Software

1. Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli Utenti dovranno ottenere espressa autorizzazione del Titolare per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria ("freeware" o "shareware").
2. Il Titolare richiama l'attenzione del proprio personale su alcuni aspetti fondamentali che l'Utente è tenuto ad osservare per un corretto utilizzo del software in azienda:
 - a. il Titolare acquista le licenze d'uso dei software da vari fornitori esterni. L'Utente, pertanto, è 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 contratti di licenza;
- b. non è consentito fare né il download né l'upload tramite internet di software non autorizzato;
 - c. il Titolare, sulla scorta di quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, ricorda che le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi possono essere condannate al pagamento dei danni e anche alla reclusione;
 - d. in nessun caso il Titolare utilizza software o altri strumenti di tipo Key Log per la registrazione delle operazioni eseguite da tastiera;
 - e. il Titolare non tollererà la duplicazione illegale del software.

Articolo 11 - Dispositivi di memoria portatili

1. L'utilizzo di dispositivi di memoria portatili risponde alle direttive che di seguito si riportano:
 - a. non è consentito utilizzare supporti rimovibili personali per lo scambio dati, se non preventivamente autorizzati per iscritto dal Titolare; è onere dell'Utente custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato e/o alterato e/o distrutto.
 - b. Ove autorizzati in base a quanto sopra disposto, una volta connessi all'infrastruttura informatica del Titolare, i dispositivi saranno soggetti (ove compatibili) al presente Regolamento.

Articolo 12 - Stampanti e fotocopiatrici

1. L'utilizzo dei suddetti strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte del Titolare.

2. È richiesta una particolare attenzione quando si invia su una stampante condivisa documenti aventi ad oggetto dati personali o informazioni riservate al fine di evitare che persone non autorizzate possano venirne a conoscenza. Si richiede quindi di evitare di lasciare le stampe incustodite e ritirarne immediatamente le copie non appena uscite dalla stampa.

Articolo 13 - Utilizzo di cartelle di rete nominative

1. Al personale della segreteria e ai docenti sono attribuite cartelle di rete sul server virtuale, le quali dovranno essere utilizzate per finalità esclusivamente riconducibili allo svolgimento dell'attività lavorativa. La cartella del personale amministrativo è sempre condivisa con il dirigente scolastico e con la D.S.G.A. La cartella del consiglio di classe è condivisa con i docenti dello stesso e con il dirigente scolastico.
2. La "personalizzazione" della cartella di rete non comporta la proprietà o l'usufrutto in capo alla persona autorizzata al trattamento, in quanto trattasi di strumento di esclusiva proprietà del Titolare messo a disposizione al solo fine dello svolgimento delle proprie mansioni lavorative.
3. Le informazioni ed i documenti contenuti nella cartella di rete devono essere di sola natura professionale; in caso di assenza improvvisa di un amministrativo, al fine di garantire continuità lavorativa, la D.S.G.A. gestisce l'accesso ai dati nella cartella da parte di un terzo dipendente amministrativo; al rientro l'utente verrà informato dalla D.S.G.A. in merito alle attività svolte in sua assenza.
4. I contenuti della cartella nominativa saranno conservati secondo i tempi previsti dagli obblighi contrattuali e di legge.

CAPO IV – GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Articolo 14 - Gestione utilizzo della rete internet

1. Ogni Utente potrà essere abilitato, dal Titolare, alla navigazione Internet. Con il presente Regolamento si richiama gli Utenti ad una particolare attenzione nell'utilizzo di Internet e dei servizi relativi, in quanto ogni operazione attuata è associata all'"Indirizzo Internet Pubblico" assegnato al Titolare stesso.
2. Internet è uno strumento messo a disposizione degli Utenti per uso professionale. Ciascun lavoratore, pertanto, deve quindi usare la rete Internet in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; l'Utente deve quindi prendere ogni precauzione a tale riguardo.
3. Le norme di comportamento da osservare da parte degli Utenti nell'utilizzo delle connessioni ad Internet sono le seguenti:
 - a. l'utilizzo è consentito esclusivamente per scopi istituzionali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative;
 - b. non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili;
 - c. è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
 - d. non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche o registrazioni in *guest-book*, anche utilizzando pseudonimi (o nicknames);

- e. non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- f. è consentito l'utilizzo di soluzioni di Instant Messenger e/o chat esclusivamente per scopi professionali ed attraverso gli strumenti ed i software messi a disposizione dal Titolare;
- g. non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo;
- h. non è consentito lo scambio e/o la condivisione (es. i c.d. sistemi di Peer-to- Peer) a qualsiasi titolo, anche se non a scopo di lucro, di materiale audiovisivo, cinematografico, fotografico, informatico, etc., protetto da copyright;
- i. non è consentito navigare in siti che possano rivelare una profilazione dell'individuo definita 'particolare' ai sensi del Regolamento Europeo 2016/679 (siti la cui navigazione palesi elementi attinenti fede religiosa, opinioni politiche e sindacali abitudini sessuali del dipendente);
- j. non è consentito lo scarico di software gratuiti trial, freeware e shareware;
- k. non è consentito lo scarico di materiale digitale tutelato dalle normative sul Diritto d'Autore, fatto salvo specifiche esigenze di lavoro che lo richiedano);

- l. non è permessa la partecipazione a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nickname);
 - m. non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà del Titolare in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata approvata espressamente.
 - n. È proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere nocivo all'immagine del Titolare. Queste azioni, anche se svolte da profili personali e/o al di fuori dell'orario di servizio possono far scattare provvedimenti disciplinari.
4. Per facilitare il rispetto delle già menzionate regole, il Titolare si riserva, per mezzo dell'amministratore di sistema, la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (es. upload, restrizione nella navigazione, download di *file* o software).
5. L'eventuale conservazione di dati è effettuata per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza. I sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei log file) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Articolo 15 - Gestione e utilizzo della posta elettronica istituzionale

Principi guida

1. Ad ogni Utente titolare di un account, il Titolare provvede ad assegnare una casella di posta elettronica individuale del tipo:
 - a. per i dipendenti: nome.cognome@istitutosalutaticavalcanti.it;
 - b. per le famiglie: nome.cognome.alu@istitutosalutaticavalcanti.it;
 - c. per gli ospiti: nome.cognome.guest@istitutosalutaticavalcanti.it;
 - d. per i componenti del consiglio di Istituto:
nome.cognome.cdi@istitutosalutaticavalcanti.it;
2. Quando necessario, su richiesta motivata della famiglia indirizzata al dirigente scolastico, potrà essere rilasciato una seconda mail per le famiglie, del tipo: Nome.cognome.alu.1@istitutosalutaticavalcanti.it.
3. I servizi di posta elettronica devono essere utilizzati a scopo professionale/istituzionale; l'account e-mail di servizio è uno strumento di proprietà del Titolare ed è conferito in uso per l'esclusivo svolgimento delle mansioni lavorative/istituzionali affidate. Le famiglie, a cui sono consegnate le credenziali di accesso alle piattaforme di istituto, sono le uniche responsabili degli account forniti dall'istituto e della riservatezza delle proprie credenziali perché il nome dell'alunno/studente è utilizzato esclusivamente per comodità.
4. A tutela della privacy è fatto obbligo per il personale utilizzare le e-mail di servizio per le comunicazioni interne e alle famiglie. Il personale è responsabile per le informazioni fornite tramite mail in risposta a indirizzi e-mail non di servizio. Attraverso l'e-mail istituzionale, il personale rappresenta pubblicamente il Titolare e per questo motivo viene richiesto

di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere una immagine positiva dell'Istituto;

5. A tutela della privacy è fatto obbligo alle famiglie di utilizzare la mail di servizio fornita dal Titolare per le comunicazioni formali all'Istituto e per ogni richiesta o comunicazione che riguardi il figlio.
6. Gli Utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica istituzionale e sono tenuti ad utilizzarla in modo conforme alle presenti regole. Gli stessi, pertanto, devono:
 - a. conservare la password nella massima riservatezza e con la massima diligenza;
 - b. mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti. Il limite della dimensione della casella postale è fissato in 1000Gb per Utente;
 - c. 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 (es. virus).
 - d. accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i file attachment di posta elettronica prima del loro utilizzo;
 - e. rispondere ad e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
 - f. collegarsi a siti internet contenuti all'interno di messaggi solo quando vi sia comprovata sicurezza sul contenuto degli stessi.

7. L'utente che riceve una e-mail a carattere, violento, razzista o pornografico, o che rappresenti forme di spamming o phishing ha il dovere di avvertire rapidamente il Titolare affinché siano prese le misure necessarie per fermare il ricevimento di questi messaggi non sollecitati. È vietato trasmettere e-mail di tipo professionale al proprio indirizzo privato.
8. Non è consentito agli Utenti utilizzare la casella di posta elettronica istituzionale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, etc., salvo che questo non sia funzionale all'attività prestata in favore dell'Ente (es: presentazioni o materiali video istituzionali). Si ricorda che, 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".
9. Occorre inoltre 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 nell'organizzazione di appartenenza del mittente.
10. Rispetto all'utilizzo della posta elettronica certificata si applicano, ove compatibili, le presenti disposizioni.

Accesso alla casella di posta elettronica del lavoratore assente

11. Saranno messe a disposizione di ciascun Utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le coordinate di altro

soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza del lavoratore.

12. Nel caso, invece, il Titolare necessita conoscere il contenuto dei messaggi di posta elettronica dell'Utente resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:

- a. la verifica del contenuto dei messaggi sarà effettuata per il tramite idoneo "fiduciario", da intendersi quale lavoratore previamente nominato e/o incaricato (per iscritto) dall'Utente assente;
- b. al suo rientro l'utente, il cui account sarà ceduto, sarà informato in merito alle attività svolte;
- c. sarà preventivamente richiesto all'utente di farlo lui stesso, se possibile, tramite webmail.

Cessazione dell'indirizzo di posta elettronica istituzionale

13. In caso di interruzione del rapporto di lavoro con l'Utente, l'account verrà sospeso a partire da 2 giorni lavorativi successivi di cessazione senza comunicazione da parte dell'ufficio del personale; si disporrà la definitiva e totale cancellazione dello stesso entro 24 mesi dall'interruzione del rapporto di lavoro. In ogni caso, il Titolare si riserva il diritto di conservare i messaggi di posta elettronica che riterrà rilevanti.

Articolo 16 - I controlli

1. Relativamente ai soli dipendenti, il Titolare, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Statuto dei Lavoratori), esclude la configurabilità di forme di controllo istituzionali aventi direttamente ad oggetto l'attività lavorativa dell'Utente. Ciononostante, non si esclude che, per ragioni organizzative e produttive, di tutela del patrimonio istituzionale

ovvero per esigenze dettate dalla sicurezza del lavoro, si utilizzino sistemi informatici, impianti, apparecchiature o dispositivi dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori. In tal caso tali strumenti verranno valutati e subordinati rispetto alla normativa di settore, ed i dati acquisiti con lo strumento verranno trattati secondo l'informativa privacy allegata al presente Regolamento.

2. Fermo restando il diritto del Titolare di effettuare controlli sull'effettivo adempimento della prestazione lavorativa nonché sul corretto utilizzo dei beni e servizi informatici istituzionali (artt. 2086, 2087 e 2104 c.c.), 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, nel rispetto del principio di pertinenza e non eccedenza.
3. Il Titolare, nel riservarsi il diritto di procedere a tali controlli, informa che le modalità di effettuazione degli stessi sono ispirate al principio della "gradualità" così come di seguito più precisamente specificato.

Modalità di effettuazione dei controlli

4. I controlli consentono al Titolare di intervenire con verifiche qualora si riscontrino anomalie d'area o di unità, senza arrivare, almeno in una prima fase, al dettaglio del singolo soggetto.

Secondo il principio della gradualità:

- a. I controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura istituzionale ovvero a singole aree lavorative, aventi caratteristiche tali da precludere l'immediata identificazione dell'utente.

- b. Nel caso in cui si dovessero riscontrare violazioni del presente disciplinare interno, 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 istituzionali, con conseguente invito ad attenersi scrupolosamente alle istruzioni ivi impartite.
- c. In caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

I controlli non autorizzati

- 5. In ogni caso il 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:

- a. 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;
- b. la riproduzione e la memorizzazione sistematica delle pagine internet visualizzate da ciascun Utente, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;
- c. la lettura e la registrazione dei caratteri inseriti dal lavoratore tramite tastiera o dispositivi analoghi;
- d. l'analisi occulta di computer portatili affidati in uso.

Articolo 17 - Sanzioni

1. L'eventuale violazione di quanto previsto dal presente Regolamento – rilevante anche ai sensi degli art. 2104 e 2105 c.c. - potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 dello Statuto dei Lavoratori e/ del Codice di comportamento dei dipendenti del Ministero dell'istruzione (Artt. da 12 a 16).
2. Il Titolare avrà cura di informare senza ritardo (e senza necessità di preventive contestazioni e/o addebiti formali) le autorità competenti, nel caso venga commesso un reato, o la cui commissione sia ritenuta probabile o solo sospettata, tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici istituzionali.
3. In caso di violazione accertata da parte degli Utenti delle regole e degli obblighi esposti in questo Regolamento, il Titolare si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici.
4. Nel caso specifico degli studenti, le attività svolte con l'account fornito dall'istituto concorrono alla valutazione delle competenze ad alla redazione dei documenti di valutazione, sono oggetto di valutazione da parte dei singoli docenti e degli organi collegiali e devono essere considerati attività didattiche a tutti gli effetti. A queste attività si applicano a pieno i regolamenti già previsti per la didattica in presenza.
5. Nel caso di violazioni della legge (violazione della privacy, atti di cyberbullismo, ecc.) il personale scolastico venuto a conoscenza del reato, in qualità di pubblico ufficiale, è tenuto alla denuncia alla pubblica sicurezza.

TITOLO VI — DISPOSIZIONI GENERALI E FINALI

Articolo 18 – Disposizioni finali e transitorie

1. Il presente Regolamento recepisce le disposizioni della normativa presente al gennaio 2025
2. Il presente Regolamento sopprime e sostituisce il regolamento: **REGOLAMENTO PER L'UTILIZZO DELLA STRUMENTAZIONE INFORMATICA ISTITUZIONALE E DELLA RETE INTERNET PER LA TUTELA DELLA PRIVACY.**
3. Eventuali sopravvenienze normative sono recepite automaticamente nelle parti imperative.

Articolo 19 - Comunicazioni

1. Il presente Regolamento è messo a disposizione degli Utenti, per la consultazione, al momento dell'assegnazione di un account Utente all'indirizzo web: <https://www.istitutosalutaticavalcanti.edu.it/regolamenti/>.
2. Ad ogni aggiornamento del presente documento, ne sarà data comunicazione sulle bacheche istituzionali e/o tramite l'invio di apposito messaggio e-mail. Tutti gli Utenti sono tenuti a conformarsi alla versione più aggiornata del presente Regolamento.
3. Le autorizzazioni e/o concessioni richieste dal presente Regolamento, ovvero poste nella facoltà degli Utenti, potranno essere comunicate al Titolare per mezzo di qualsiasi strumento che ne garantisce la tracciabilità (es: e-mail).