Istituto Comprensivo Statale di Sant'Angelo di Piove
Via Roma, 21 - 35020 Sant'Angelo di Piove di Sacco (PD)
tel 0495846029 c.f. 80016280283
www.icsantangelodipiove.edu.it
peo: pdic82700n@istruzione.it pec: pdic82700n@pec.istruzione.it

REGOLAMENTO INFORMATICO

Art. 1 - Premessa

Premesso che l'utilizzo delle risorse informatiche e telematiche istituzionali deve sempre ispirarsi ai principi di diligenza e correttezza, atteggiamenti questi destinati a sorreggere ogni atto o comportamento posto in essere nell'ambito del rapporto di lavoro, si ritiene utile adottare ulteriori regole interne dirette ad evitare comportamenti inconsapevoli e/o scorretti. Inoltre, questo regolamento è obbligatorio a partire dal Provvedimento dell'Autorità Garante per la Privacy del 1° marzo 2007 (Gazzetta Ufficiale n. 58 del 10 marzo 2007) e risponde anche all'esigenza di dare una corretta informativa sull'uso dei dati automaticamente ed implicitamente "trattati" a causa dell'uso di un apparato mobile (Tablet, Smartphone o Telefono cellulare).
Ai sensi del GDPR 2016/679 e della normativa nazionale vigente in materia di trattamento e protezione dei dati, ogni incaricato del trattamento, cui sia stato dato accesso al sistema informativo istituzionale mediante credenziali di autenticazione, è autorizzato all'utilizzo della strumentazione elettronica in dotazione all'Istituto (computer, stampanti, fax, scanner, fotocopiatori, dispositivi di rete, etc.) e all'utilizzo della strumentazione telefonica e di comunicazione mobile (telefoni cellulari, smartphone e tablet) per lo svolgimento dei compiti assegnati e in particolare per il trattamento dei dati personali entro il proprio ambito e secondo le istruzione ricevute.
Il presente Regolamento integra il vigente Disciplinare interno e policy istituzionale sul trattamento dei dati.

Art. 2 - Destinatari

Il presente Regolamento si applica a tutti gli attori dell'Istituto, ivi compreso il personale Docente e ATA nonché i visitatori. Da Regolamento di Istituto, agli alunni non è consentito l'utilizzo del telefono cellulare. Fanno eccezione gli eventuali strumenti digitali compensativi speciali che, su richiesta delle singole famiglie e su indicazione medica, verranno valutati preventivamente dal team dei Docenti/Consiglio di Classe.
È fatta eccezione per il Dirigente Scolastico e per i responsabili dei plessi, nonché per i collaboratori, ai rispettivi diversi livelli, del Dirigente Scolastico, che sono autorizzati al loro utilizzo per ragioni logistiche ed organizzative.

2.1 Docenti, personale amministrativo, collaboratori scolastici

Il personale, ad eccezione delle figure richiamate al paragrafo precedente, quando svolge l'attività lavorativa è tenuto ad attivare la modalità silenziata sul proprio dispositivo e a non utilizzare il proprio dispositivo personale, fatta eccezione per comprovate urgenze. In particolare i docenti, durante le lezioni, al fine di non disturbare lo svolgimento delle stesse.

2.2 Genitori

Non violano la privacy le riprese video e le fotografie raccolte dai genitori, durante le recite e i saggi scolastici. Le immagini, in questi casi, sono raccolte per **esclusivi fini personali** e destinate a un ambito familiare o amicale, ma **non** alla **diffusione**. Relativamente alle registrazioni audio/video in contesti diversi da quelli evidenziati, queste sono consentite esclusivamente nei casi e con le modalità previste dalla normativa vigente.

2.3 Visitatori

L'uso del cellulare o altro dispositivo elettronico equivalente per la realizzazione di fotografie, video, registrazioni audio è **tassativamente vietato** se non espressamente e preventivamente autorizzato dal Dirigente Scolastico, e comunque al di fuori dei casi previsti dalla normativa vigente.

Art. 3 - Utilizzo del dispositivo mobile

3.1 Disposizioni generali

3.1.1. Per "Dispositivo mobile", ai fini del presente articolo, si intende il tablet o altro strumento mobile in dotazione da parte dell'istituzione scolastica per fini lavorativi. Attualmente, gli unici dispositivi mobili in dotazione sono i tablet.

Le seguenti disposizioni non si applicano ai dispositivi personali dei docenti, per i quali valgono norme specifiche indicate in articoli successivi del presente regolamento.
In generale, i dispositivi mobili non possono essere ceduti né fatti utilizzare a terzi, eccetto colleghi, collaboratori, consulenti o soggetti autorizzati.
3.1.2. Il Responsabile IT (Information Technology) può disporre dei dispositivi mobili secondo necessità, sostituendo, aggiornando, rimuovendo o adeguando in tutto o in parte le componenti hardware e/o software di cui essi si compongono, senza necessità di preavviso e di richiesta di consenso da parte dell'utilizzatore. Il Responsabile IT è l'unico che può provvedere o autorizzare l'installazione, l'aggiornamento e la configurazione di dispositivi hardware e/o software sui programmi in uso, sui dispositivi mobili.
3.1.3. Non è consentito modificare le caratteristiche hardware e software impostate sui dispositivi mobili. Non è consentita l'installazione di programmi diversi da quelli autorizzati. Non è consentita la riproduzione, la duplicazione, il salvataggio o lo scarico (download o file sharing) di programmi o file di ogni tipo (testo, immagini, video, audio, eseguibili) in violazione delle norme sul diritto d'autore, ai sensi delle Legge n. 128 del 21 maggio 2004.
Non è consentita l'installazione di ulteriori dispositivi rispetto a quelli in dotazione.
Non è consentito l'uso di qualsiasi dispositivo esterno collegabile al dispositivo mobile, se non quelli istituzionali o quelli autorizzati.
L'utilizzatore che abbia necessità di apportare modifiche software o hardware al dispositivo mobile in dotazione, installando nuovi programmi o dispositivi, deve farne preventiva richiesta al Responsabile IT.
Quanto memorizzato sui supporti interni al dispositivo mobile potrebbe essere oggetto di analisi, controllo e duplicazione da parte del Responsabile IT o da personale tecnico autorizzato, per migliorare l'affidabilità, la disponibilità e l'efficienza del dispositivo.
Qualora fossero individuate componenti hardware e/o software (programmi, documenti, dispositivi esterni, etc.) non corrispondenti ai criteri di sicurezza e di operatività individuati dal Responsabile IT o non esplicitamente autorizzati, tali componenti potrebbero essere rimossi e l'utilizzatore potrebbe essere coinvolto negli accertamenti e nelle verifiche del caso.

3.2 Disposizioni operative

3.2.1. I dispositivi mobili devono avere abilitato il codice di blocco e/o il PIN d'accesso e/o la Password personalizzata. Tale codice d'accesso dev'essere impostato al massimo del numero di caratteri consentito dal sistema operativo dello strumento e l'eventuale password utilizzata non deve facilmente richiamare né date di nascita né altri riferimenti anagrafici. Si consiglia l'uso di password alfanumeriche composte anche di lettere maiuscole e simboli (14 caratteri alfanumerici e speciali), sempre se ammessi dal sistema operativo del dispositivo mobile in dotazione.
Il Bluetooth ed ogni altro protocollo che consenta l'associazione di dispositivi diversi dallo strumento mobile, deve essere abilitato per l'accoppiamento ai soli strumenti istituzionali in dotazione. Inoltre può essere usato, in particolare, per l'attivazione dell'auricolare personale e/o del kit viva-voce dell'auto. Il Bluetooth non va mai lasciato inutilmente attivo e le password di associazione non devono mai essere quelle di default previste per il dispositivo.

3.3 Uso del cellulare o altro dispositivo elettronico equivalente atto a ricevere/inviare telefonate, videochiamate, sms, mms, registrare audio e video, fotografare, utilizzare chat e social network, collegarsi alla rete intranet e/o internet, e comunque per altri scopi non riconducibili all'attività didattica prevista nel Piano dell'Offerta Formativa dell'Istituto.

Limitatamente al personale, si ribadisce la puntuale applicazione della normativa vigente (DPR 249/1998, DPR 235/2007, Direttiva Ministeriale n. 30 del 15 marzo 2007 e Direttiva Ministeriale n. 104 del 30 novembre 2007), pertanto l'uso del cellulare e degli altri dispositivi equivalenti per finalità non riconducibili all'attività didattica prevista dal Piano dell'Offerta Formativa non è consentito.

3.4 Uso del cellulare o altro dispositivo elettronico equivalente atto a ricevere/inviare telefonate, videochiamate, sms, mms, registrare audio e video, fotografare, utilizzare chat e social network, collegarsi alla rete intranet e/o internet,

e comunque per altri scopi riconducibili all'attività didattica prevista nel Piano dell'Offerta Formativa dell'Istituto.
Limitatamente al personale ed agli studenti, l'uso dei dispositivi mobili può essere eventualmente consentito nella classi della scuola Secondaria di primo grado, e solo in casi particolari (es. strumenti compensativi certificati) anche nella Scuola dell'Infanzia e Primaria, preventivamente concordati ed autorizzati dal Dirigente Scolastico e/o dal Consiglio di Classe, o qualora servisse per lo svolgimento di attività didattiche, previste all'interno del Piano dell'Offerta Formativa, particolarmente innovative e collaborative, che prevedano anche l'uso di dispositivi tecnologici, compresa l'acquisizione da parte degli studenti di un elevato livello di competenza digitale, soprattutto per quanto riguarda l'uso consapevole e responsabile delle tecnologie. Si ricorda che la competenza digitale è una delle competenze chiave, per l'apprendimento permanente, identificate dall'Unione Europea. L'uso di smartphone, tablet e altri dispositivi mobili, o delle funzioni equivalenti presenti sui telefoni cellulari è pertanto consentito, ma unicamente su indicazione del docente, esclusivamente per finalità didattiche previste nel Piano dell'Offerta Formativa, in momenti ben definiti e con modalità prescritte dall'insegnante, con comunicazione scritta alle famiglie.
In ogni caso il ricorso ai predetti strumenti personali per la realizzazione di fotografie, registrazioni audio/video che comportino il trattamento di dati personali è da considerarsi vietato, in favore di tecnologie più tutelanti (es.: apparecchi foto/video grafici quali fotocamere, videocamere, ecc.).

Art. 4 Utilizzo delle aule informatiche
4.1 Prenotazione
I docenti che intendono utilizzare l'aula informatica per i ricevimenti a distanza, ove previsti, sono tenuti a effettuare la prenotazione attraverso il sistema di gestione delle prenotazioni dell'Istituto.
In caso di indisponibilità del sistema, la prenotazione dovrà essere effettuata in accordo con il Responsabile IT del plesso.
La sala informatica resta costantemente chiusa a chiave; la chiave deve essere richiesta ai collaboratori scolastici.
4.2 Orari di Utilizzo
L'accesso all'aula informatica è consentito esclusivamente negli orari di apertura dell'Istituto, come stabilito dal calendario scolastico.
4.3 Prenotazione per Attività Didattiche
La prenotazione dell'aula informatica, del carrello con PC portatili e dei tablet per attività didattiche avviene tramite Google Calendar, utilizzando le credenziali istituzionali.
4.4 Risorse disponibili in ogni plesso sono:
"Aula"
"Tablet "
"Carrello"
I docenti devono verificare la disponibilità delle attrezzature e prenotare la fascia oraria desiderata.
4.5 Riservatezza e Protezione dei Dati durante il ricevimento dei genitori a distanza
Durante i ricevimenti online, il docente è responsabile della protezione dei dati personali degli studenti, con particolare attenzione a informazioni sensibili, valutazioni scolastiche e documentazione riservata.
È vietato lasciare documenti riservati, appunti o materiali personali salvati o aperti sui computer dell'aula informatica.
4.6 Accesso e Sicurezza Informatica
I docenti devono accedere ai dispositivi informatici utilizzando il proprio account istituzionale personale.
È vietata la condivisione delle credenziali di accesso.
La connessione a Internet è autorizzata solo tramite il proprio account e solo per fini strettamente istituzionali.

Ogni allievo deve utilizzare il codice assegnato, identificabile tramite un numero corrispondente al proprio numero di registro scolastico. Questa assegnazione consente il tracciamento delle attività e garantisce una gestione ordinata delle postazioni.
Ogni docente e ogni alunno hanno accesso al proprio account GSuite attivato dall'Istituto.
Si ricorda che durante l'utilizzo dei computer restano memorizzate alcune tracce delle attività svolte (cronologia di navigazione, file creati, password, compilazione di moduli, ecc.). Per questo motivo, è importante accedere sempre con il proprio account personale e fare logout al termine della sessione.

4.7 Comportamento nell'Aula

È richiesto un comportamento professionale e rispettoso nei confronti di colleghi, studenti e personale scolastico.
È vietato consumare cibi o bevande nell'Aula informatica, per garantire la conservazione delle attrezzature.

4.8 Segnalazione di Malfunzionamenti

Qualsiasi malfunzionamento o guasto tecnico deve essere segnalato tempestivamente al personale tecnico o all'amministrazione.
Al termine dell'utilizzo, il docente deve: spegnere tutte le apparecchiature utilizzate e lasciare l'Aula in ordine.

4.9 Responsabilità

Il docente è responsabile dell'Aula e delle attrezzature per tutta la durata della prenotazione.
In caso di danni non segnalati, sarà ritenuto responsabile il docente risultante dall'ultima prenotazione registrata.

4.10 Uso Condiviso e Rispetto degli Orari

È obbligatorio rispettare l'orario prenotato e liberare la sala puntualmente. L'uso dell'aula senza prenotazione non è consentito. La disposizione dei pc non va assolutamente modificata ed il docente deve controllare che banchi e sedie siano rimessi in ordine al termine delle attività.
Il docente deve utilizzare il computer collegato alla LIM. Da questa postazione è possibile:

- monitorare i desktop degli studenti;
- inviare messaggi personalizzati;
- condividere il proprio schermo;
- trasferire file;
- prendere il controllo dei dispositivi degli alunni per fornire supporto operativo o risolvere eventuali problemi.

Al termine della lezione, il docente è tenuto a verificare che tutti i computer siano spenti, che la LIM sia spenta, così come la ciabatta generale a cui è collegata.

4.11 Sicurezza dei Dati

Al termine della sessione, i docenti devono effettuare il logout dai propri account.
È fortemente sconsigliato salvare dati personali sui dispositivi. È inoltre buona prassi cancellare la cronologia del browser.
È vietato scaricare materiale da internet non legato alla didattica, in ogni caso è da tenere sempre presente la legislazione in materia di copyright e diritto d'autore.
In caso di fruizione di contenuti internet (pagine web e/o video online), per l'attività didattica in presenza degli alunni, i contenuti stessi devono essere preventivamente controllati da parte del docente per accertarsi che siano adatti agli alunni.

Art. 5 – Utilizzo delle Attrezzature in dotazione

Le strumentazioni in dotazione all'Istituto (computer, stampanti, lim, digital board e tablet) devono essere utilizzate esclusivamente per finalità istituzionali. È vietata l'installazione autonoma di software o la modifica delle impostazioni dei dispositivi senza autorizzazione tecnica.
Tablet e carrello di pc possono essere utilizzati in aula dagli alunni previa prenotazione, da effettuarsi secondo la medesima procedura prevista per l'aula informatica:

- accedere a Google Calendar con il proprio account istituzionale;
- verificare la disponibilità;

- prenotare l'orario desiderato.

Al termine dell'utilizzo, i dispositivi (tablet e PC portatili) devono essere riposti negli appositi alloggiamenti e, ove previsto, collegati alla ricarica.
È vietato portare i dispositivi all'esterno dell'Istituto senza preventiva autorizzazione scritta.
Interventi Tecnici: qualsiasi modifica, installazione o intervento tecnico deve essere richiesto al personale tecnico dell'Istituto. È severamente vietato effettuare interventi tecnici in autonomia.

Art. 6 – Formazione

I docenti che necessitano di supporto possono richiedere formazione sull'uso delle attrezzature o sulle modalità di prenotazione, rivolgendosi al responsabile tecnico del plesso.
Per ulteriori informazioni o per segnalazioni tecniche, rivolgersi al responsabile tecnico dell'Istituto.

Art. 7 - Guasto o furto

In caso di guasti o malfunzionamenti, l'utilizzatore dovrà rivolgersi al Responsabile IT a cui è demandata la relativa gestione in queste circostanze.
In caso di furto o smarrimento o danneggiamento dei dispositivi mobili, l'utilizzatore deve dare tempestiva comunicazione al Responsabile IT, rimanendo a disposizione nel caso sia necessario denunciare l'accaduto all'Autorità preposta.
Non è esclusa a priori la responsabilità dell'utilizzatore nel sostenere, anche solo in parte, i costi per la riparazione o sostituzione del dispositivo mobile.

Art. 8 - ACCESSO AL SERVIZIO WI-FI

8.1 Norme generali sull'attività di navigazione

Si prevede il regolare utilizzo nei locali dell'Istituto di dispositivi con cui i docenti e il personale ATA possono collegarsi alla rete WIFI dell'Istituto e, tramite questa, a internet. L'accesso a internet avviene attraverso un filtro per la navigazione che limita, per quanto possibile, la possibilità di accedere a materiale inadeguato e/o illegale su internet.
Gli utenti che accedono a Internet attraverso i sistemi messi a disposizione dall'Istituto sono tenuti ad usare questa risorsa in modo corretto e responsabile, in accordo con gli scopi educativi, informativi e istituzionali per i quali è fornita. L'utente si impegna, di conseguenza, ad utilizzare il servizio WI-FI erogato dall'Istituto, nel pieno rispetto della legislazione vigente e del Codice di Comportamento Nazionale. In particolare l'uso responsabile e corretto di internet comporta il formale impegno a:
-riconoscere che la scuola, tramite il servizio WiFi fornito, non è responsabile in alcun modo per il contenuto, la qualità, la validità di qualsiasi informazione reperita in rete;
-astenersi da un uso di Internet per scopi vietati dalla legislazione vigente nonché dal presente Regolamento o per scopi difformi da quelli didattici e formativi previsti nel PTOF e comunque sempre con la diligenza del buon padre di famiglia;
-non recare disturbo o danno agli altri utilizzatori della Rete tramite l'invio di messaggi di posta elettronica commerciali, propagandistici o pubblicitari;
-non compiere azioni di mail indiscriminate (spamming);
-non effettuare operazioni di condivisione di files (peer to peer) in quantità e per dimensioni tali da compromettere il buon uso, agli altri utenti, della rete;
-assumersi la totale responsabilità per il contenuto dei messaggi eventualmente trasmessi e, più in generale, per l'uso del servizio;
-assumersi la totale responsabilità per eventuali minacce, relative a virus e malware che possano, in tutto e/o in parte, compromettere il normale uso della rete, dovuti alla propria navigazione in internet o ai propri ai propri dispositivi personali connessi alla rete;
-assumersi la totale responsabilità per il software presente nel proprio dispositivo che possa, in tutto e/o in parte, compromettere il normale uso della rete, o arrecare danno agli altri utenti e/o alla scuola;

-osservare le leggi vigenti in materia di diritto d'autore e tutela della privacy, nonché le specifiche norme penali relative al settore informatico e della comunicazione elettronica, oltre ad ogni altra disposizione generale di Legge;
-non accedere a siti che per contenuti ed immagini siano in contrasto con le finalità scolastiche del servizio o comunque non preventivamente autorizzati dal Dirigente Scolastico o dal responsabile Tecnico;
-sollevare l'Istituto da qualsiasi responsabilità per qualsiasi evento subito o arrecato a terzi con l'uso del servizio Hot Spot WiFi.
- non ricercare, scaricare o caricare informazioni, applicazioni, files multimediali o documenti che, per tipologia, caratteristiche e/o dimensione, possano, ai sensi della normativa vigente, arrecare danno alla scrivente e/o a terzi, inclusa la compromissione, totale e/o parziale del servizio.
Qualora dovesse essere rilevato un uso difforme dal presente regolamento e da quanto previsto dalle vigenti Leggi, gli utenti che risulteranno responsabili di tali accessi verranno immediatamente disabilitati all'accesso, e verranno applicate le eventuali sanzioni previste in tali casi, oltre alla comunicazione, in modo riservato, dei reati presso le competenti sedi civili e penali, unitamente ai log dei transiti, ai siti collegati, alle immagini richiamate con il nominativo dell'utente e quant'altro venisse richiesto dalle Autorità competenti.

8.2 Registrazione ed accesso al servizio

L'utilizzo della rete wifi è ad uso esclusivo di docenti e personale ATA; ogni utente riceverà una username ed una password per l'utilizzo del servizio e per l'accesso ai dispositivi elettronici presenti nelle aule; username e password sono di proprietà dell'Istituto e su di esse grava l'obbligo di conservazione da parte dell'utente.
L'accesso alla rete WiFi durerà fino a scadenza del contratto per il personale.
La connessione, nelle zone coperte dal segnale, sarà attiva 24h su 24h, fatte salve interruzioni derivanti da necessità di manutenzione degli apparati o di altra natura non dipendenti dalla volontà dell'Amministrazione.
L'indebita cessione o utilizzo delle credenziali a terzi comporta l'immediata esclusione dal servizio, fatte salve eventuali maggiori responsabilità che la normativa vigente ponga a carico dell'utente.
L'utente che ha ottenuto l'accesso ha la totale responsabilità delle attività svolte per il tempo di utilizzo del servizio.

8.3 Misure di sicurezza

Per il corretto utilizzo del servizio e per garantire la necessaria sicurezza e riservatezza della rete WiFi, ogni utilizzatore si dovrà impegnare a:

- utilizzare un solo dispositivo per la connessione alla rete WiFi, oltre ai dispositivi presenti in Istituto;
- provvedere ad installare, nel proprio dispositivo, un adeguato software antivirus, aggiornabile automaticamente (anche gratuito), a non disabilitarlo durante la fruizione del servizio, e a verificarne la corretta operatività;
- il log-out dalla rete WiFi avviene automaticamente dopo 8 ore;

8.4 Limitazioni del servizio ed esclusioni di responsabilità

L'Istituto, in forza della gratuità dell'iniziativa, pur impegnandosi a fornire un servizio della massima qualità, non si assume responsabilità per la qualità del segnale e la piena copertura delle zone indicate.
Gli strumenti per l'accesso al servizio (portatili, smartphone, tablet, ecc.), ove non diversamente stabilito, non sono forniti dall'Istituto ed il loro utilizzo per l'accesso alla rete internet attraverso il WiFi della scuola avviene sotto l'esclusiva responsabilità del proprietario/utilizzatore.
L'utente non può cedere a terzi la connettività o fare un qualsiasi uso commerciale del servizio.
Non è consentito lo scarico di immagini, filmati e files musicali non attinenti all'attività lavorativa ed in violazione delle leggi sul diritto d'autore.

8.5 Posta elettronica istituzionale

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

- le caselle di posta elettronica istituzionale assegnate ai dipendenti ed ai collaboratori sono del tipo cognome.nome@icsantangelodipiove.edu.it;
- la natura della corrispondenza effettuata con le caselle di posta elettronica istituzionali non è privata e non è consentito utilizzare tali caselle per motivi non attinenti allo svolgimento delle mansioni assegnate; i responsabili sono tenuti a controllare la posta in arrivo almeno una volta al giorno e devono delegare una persona di fiducia che possa farlo in caso di propria assenza;
- non è consentito inviare o memorizzare messaggi di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- tutte le caselle di posta elettronica sono oggetto di salvataggio automatico sia per le comunicazioni in ingresso che in uscita.

Art. 9 Sanzioni

9.1 Limitatamente agli alunni si rinvia al Regolamento di Istituto.

Per quanto riguarda i Docenti e il personale per la realizzazione di riprese audio/foto/video al di fuori dei contesti formativi previsti nel PTOF, realizzazione di riprese audio/foto/video senza preventiva autorizzazione, da parte degli interessati, diffusione di riprese audio/foto/video tramite social, servizi di messaggistica istantanea, internet, altri media e servizi informatici di pubblicazione, realizzazione di riprese audio/foto/video durante riunioni degli organi collegiali senza preventiva autorizzazione, ove prevista per Legge, si rinvia alla normativa giuslavoristica e privacy.

9.2 Cyberbullismo

Come espresso nel Regolamento di Istituto, si richiama l'attenzione degli studenti e delle rispettive famiglie, e dei docenti sulle possibili conseguenze di eventuali riprese audio/video o fotografie effettuate all'interno degli ambienti scolastici, al di fuori dei casi consentiti, e successivamente diffuse con l'intento di ridicolizzare compagni, insegnanti o colleghi, o addirittura allo scopo di intraprendere azioni riconducibili a fenomeni di cyberbullismo. Tali azioni possono configurare, nei casi più gravi, gli estremi di veri e propri reati.

La scuola, nella persona del Dirigente Scolastico, informerà tempestivamente i responsabili (o chi ne esercita la responsabilità genitoriale), qualora venga a conoscenza di atti di cyberbullismo; i comportamenti, accertati, che si configurino come forme di cyberbullismo verranno considerati come infrazione gravi.

Colui il quale commette atti di cyberbullismo sarà soggetto a provvedimenti di natura civile e penale così come stabilito dalle norme in premessa.

Gli episodi di cyberbullismo saranno perseguiti con sanzioni particolarmente incisive per i fatti di estrema gravità, secondo le previsioni del Regolamenti di Istituto .

Verranno considerate al pari di chi commette atti di cyberbullismo le condotte dei compagni sostenitori di tali comportamenti, perché, pur non partecipando direttamente alle prevaricazioni, con il loro assenso contribuiscono a rafforzare il comportamento lesivo della dignità e dell'incolumità psicofisica delle vittime.

Art. 10 - Iniziative scolastiche

La scuola promuove iniziative di informazione e formazione sui temi dell'uso consapevole dei dispositivi informatici, dei nuovi media, dei social network e in generale delle applicazioni web e mobili. Tali iniziative sono rivolte principalmente agli alunni ed al personale, ma anche, ove possibile, alle famiglie.

Art. 11. Controlli e tutela della privacy

11.1 Poiché in caso di violazioni contrattuali e giuridiche, sia l'Istituto, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Istituto verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

Ai sensi dell'art. 13 e 14 del GDPR 2016/679 e della normativa nazionale vigente, in conformità a quanto disposto dalla Provvedimento n. 13 del 1° marzo 2007 dell'Autorità Garante per la privacy, si ritiene necessario informare che:

- la Direzione, attraverso l'Area IT istituzionale, effettua un monitoraggio periodico dell'hardware e del software installato nei dispositivi istituzionali. Tale operazione viene effettuata, in modo completamente automatico per i dispositivi ed i sistemi operativi che lo consentono ed in modo manuale per tutti gli altri. Il monitoraggio, necessario per finalità organizzative (inventario del parco macchine e contabilità delle licenze d'uso del software), non coinvolge in alcun modo i dati personali;
- al fine di prevenire, per quanto e ove possibile, comportamenti scorretti durante la navigazione in Internet, l'Istituto si avvale di appositi filtri che impediscono l'accesso a siti non ritenuti idonei ed il download di files multimediali non attinenti all'attività lavorativa;
- eventuali comportamenti anomali saranno segnalati genericamente alle aree interessate (uffici, servizi) e, solo qualora tali comportamenti dovessero continuare, la Direzione potrà procedere, nel rispetto delle norme legali e contrattuali, a controlli individuali;
- nessun controllo viene effettuato sui messaggi di posta elettronica il cui contenuto riguarda forme di corrispondenza assistite da garanzie di segretezza, tutelate anche dalla Costituzione e da norme penali.

11.2 Il trattamento dei dati, così come descritto, è obbligatorio, pena l'impossibilità di utilizzare qualunque dispositivo mobile.
I dati personali saranno trattati nel rispetto delle modalità indicate nel GDPR 2016/679, il quale prevede, tra l'altro, che i dati stessi siano trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi determinati, espliciti e legittimi, esatti, e se necessario aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità del trattamento, nel rispetto delle misure di sicurezza previste dall'art. 32 GDPR 2016/679.
I dati potranno essere comunicati in Italia e all'Estero all'interno del Gruppo Comprensivo di S. Angelo di Piove di Sacco e a soggetti terzi per incarichi specifici e rispondenti alle finalità del trattamento e nei casi previsti dalla legge.
Gli utenti possono esercitare i diritti di cui agli artt. dal 15 al 22 del GDPR 2016/679, tra cui conferma dell'esistenza, rettifica, integrazione e cancellazione dei dati.
Titolare del trattamento è l'Istituto Comprensivo di S. Angelo di Piove di Sacco.

Art. 12. Aggiornamento e revisione del regolamento

Il presente regolamento entra in vigore il 01/09/2025 e cessa di avere validità nel momento in cui verrà emanato un nuovo regolamento. Il presente regolamento verrà aggiornato in caso di nuove normative o evoluzioni tecnologiche.

Approvato dal Collegio dei Docenti nella riunione del 27/06/2025 e adottato dal Consiglio di Istituto con Delibera n. 86 dell'01/07/2025.