ISTITUTO COMPRENSIVO VILLA LAGARINA

E-policy: sicurezza in rete

Indice

Introduzione

La presenza sempre più diffusa delle tecnologie digitali nella vita di tutti i giorni dei più giovani, compresi gli ambienti scolastici, apre nuove opportunità ma impone nuove attenzioni dal punto di vista del loro uso sicuro, consapevole e positivo. Inoltre, lo sviluppo e l'integrazione dell'uso delle Tecnologie dell'Informazione e della Comunicazione (TIC), ed in particolare di Internet, nella didattica offrono le condizioni e l'occasione per una trasformazione dell'insegnamento e dell'apprendimento nelle scuole (Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente).
E' necessario per ogni Istituto Scolastico dotarsi di una ePolicy, documento volto a promuovere le competenze digitali ed un uso delle tecnologie positivo e consapevole.
Ciò pone però delle sfide importanti, che riguardano più livelli di conoscenze, abilità e attitudini che i più giovani hanno bisogno di sviluppare, nell'ottica di accrescere le competenze digitali.
Gli adulti hanno un ruolo fondamentale nel garantire che bambini/e e adolescenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro; in tale compito sono coinvolti a pieno titolo tutti coloro che hanno un ruolo educativo, oltre che formativo, in altre parole la comunità scolastica nel suo complesso, genitori inclusi.

Nello specifico, con questo documento l'Istituto intende regolamentare:

1. l'approccio educativo alle tematiche connesse alle competenze digitali, alla sicurezza in rete, alla privacy, all'uso della tecnologia nella didattica.
2. I comportamenti e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (TIC) in ambito scolastico.
3. Le misure per la prevenzione e la sensibilizzazione di comportamenti online a rischio.
4. Le misure per la rilevazione, la segnalazione e la gestione delle situazioni pericolose legate ad un uso non corretto delle tecnologie digitali, connesse al Piano di prevenzione e contrasto del bullismo e cyberbullismo del nostro Istituto.

Scopo della ePolicy

La presente ePolicy si configura come un insieme di regolamenti, linee di azione e attività, che hanno come finalità generale quella di promuovere un **uso sicuro e responsabile della rete e delle tecnologie digitali nella didattica**, attraverso la definizione di misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nell'insegnamento e negli ambienti scolastici, azioni di prevenzione e di gestione di situazioni problematiche relative all'uso delle tecnologie digitali (*cyberbullismo, setting, grooming*, ecc.).
Il contenuto della ePolicy sarà condiviso e comunicato agli/alle alunni/e, agli operatori dell'Istituzione e alle famiglie, il Regolamento di disciplina alunni/e terrà a riferimento il contenuto della ePolicy.

Ruoli e responsabilità

Affinchè l'ePolicy sia davvero uno strumento efficace per la scuola e la comunità occorre che tutti, in base al ruolo, si impegnino nella promozione e attuazione.

Dirigente:

- garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- attivarsi affinché i docenti possano avere una formazione di base sulle TIC tale da consentire loro il possesso delle competenze necessarie all'utilizzo di tali risorse;
- garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza;
- garantire la sicurezza on-line e applicare le procedure previste dal Regolamento in caso di abusi riguardanti l'uso di Internet e delle TIC;
- favorire il coinvolgimento e la partecipazione di famiglie, studenti/esse, docenti, a momenti formativi e a progetti sul tema della sicurezza, per la realizzazione di una cultura digitale condivisa.

Tecnico di laboratorio:

- controllare il funzionamento delle attrezzature informatiche;
- gestire situazioni di profilo tecnico (diritti di accesso ai dati; restrizioni livello utente, gestione dei laboratori, software, aggiornamenti, installazioni, licenze d'uso, antivirus, ecc.);
- fornire supporto all'attività didattica nell'utilizzo delle TIC;
- collaborare con i docenti nel sorvegliare sull'uso corretto delle attrezzature nel rispetto delle normative vigenti e del Regolamento di laboratorio.

Personale amministrativo e ausiliario (ATA):

- collaborare con i docenti nel sorvegliare i comportamenti degli studenti;
- formarsi sulle tematiche bullismo e cyberbullismo;
- segnalare eventuali comportamento non adatti al Dirigente.

Animatore digitale:

- collaborare alla realizzazione del curricolo Competenze Digitali d'Istituto in accordo con il dirigente scolastico;
- elaborare per la propria scuola il documento che individua le politiche di uso accettabile delle tecnologie;
- organizzare momenti formativi all'interno del proprio Istituto e/o in ambito della rete di scuole;
- organizzare attività di educazione ai media e favorirne la partecipazione di famiglie, studenti/esse e insegnanti;
- individuare soluzioni metodologiche-didattiche e tecnologiche sostenibili e inclusive, in collaborazione con il tecnico, da diffondere all'interno della scuola;
- curare il proprio aggiornamento professionale per l'ambito di riferimento anche in contatto con altri colleghi.

Docenti:

- provvedere alla propria formazione/aggiornamento sull'utilizzo sicuro del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei

diritti dei materiali reperiti in rete e dell'immagine degli altri, prevenzione e contrasto del cyberbullismo);
- sviluppare le competenze digitali degli/delle alunni/e, formandoli ad un uso consapevole e sicuro del web e delle tecnologie digitali, sia a scuola sia nelle attività didattiche extracurricolari (per comunicazione, studio e ricerca);
- segnalare prontamente alle famiglie e al Dirigente scolastico eventuali problematiche riguardanti l'utilizzo del digitale o episodi di violazione delle norme di comportamento stabilite dalla scuola per individuare comuni linee di intervento educativo.

Alunni/e:
- ascoltare e seguire le indicazioni fornite dai docenti per un uso corretto e responsabile delle tecnologie digitali;
- seguire le regole della Epolicy per evitare situazioni di rischio;
- mantenere un comportamento rispettoso nei confronti dei compagni, degli insegnanti e delle attrezzature informatiche;
- chiedere l'intervento dell'insegnante o dei genitori o di un adulto in caso di difficoltà attraverso i canali che la scuola mette a disposizione.

Genitori:
- contribuire in collaborazione con la scuola alla sensibilizzazione dei propri figli/e sul tema della sicurezza in rete;
- agire in modo concorde con la Scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
- assistere i figli/e nel momento dell'utilizzo della rete in ambito domestico, mettendo in atto i sistemi di sicurezza che aiutino a diminuire il rischio di imbattersi in materiale indesiderato;
- partecipare ad eventi, dibattiti informativi e formativi promossi dalla scuola con il coinvolgimento di esperti, sui temi oggetto di questo documento.

Soggetti esterni che lavorano con la scuola:
- essere sensibilizzati e consapevoli dei rischi della rete in ambito scolastico;
- garantire agli studenti la sicurezza riguardo ai rischi online.

Condivisione e comunicazione dell'Epolicy

Il documento è condiviso con l'intera comunità scolastica, ponendo particolare attenzione agli studenti e alle studentesse a cui saranno specificati compiti, funzioni e attività.
Il documento, deliberato dal Collegio Docenti e dal Consiglio dell'Istituzione, viene condiviso attraverso:
- sito web istituzionale;
- bacheca cyberbullismo
- incontri informativi rivolti a studenti e famiglie (in presenza o online)

Formazione e curricolo

L'Istituto promuove l'acquisizione, lo sviluppo e il miglioramento delle competenze digitali degli/delle studenti/esse, anche con particolare riguardo all'utilizzo critico e consapevole dei social network e dei mezzi di comunicazione, nel rispetto degli altri e sapendo prevenire ed evitare i pericoli. Ciò avverrà in coerenza con il Curricolo Digitale d'Istituto,

elaborato in rete durante l'anno scolastico 2020/2021 e approvato dal Collegio Docenti nel giugno 2021.
Tutte le discipline concorrono alla costruzione della competenza digitale dell'alunno/a.
La scuola:

- provvede ad una adeguata diffusione della presente Epolicy a tutti i componenti della comunità scolastica;
- garantisce che tutto il personale sia a conoscenza delle proprie responsabilità per un uso corretto e consapevole delle tecnologie informatiche;
- assicura percorsi di formazione di rete e di informazione per tutti i componenti della comunità scolastica sulle tematiche della sicurezza informatica.

Azioni messe in atto dall'Istituto
Le azioni messe in atto annualmente dall'Istituto sono:

- un percorso di Accoglienza Digitale ed alfabetizzazione per i nuovi docenti; il percorso viene attivato nelle prime settimane di settembre ed eventualmente, se necessario, ad ogni nuovo ingresso;
- un percorso di aggiornamento sull'uso degli strumenti di gestione: Registro Elettronico;
- un percorso di aggiornamento relativo all'utilizzo degli strumenti digitali didattici: Google Workspace.
- un percorso relativo alle metodologie didattiche che integrino il digitale nei curricoli delle varie discipline
- un percorso relativo alla gestione dei documenti scolastici (drive condiviso e documenti condivisi)

Sensibilizzazione delle famiglie e integrazione al Patto di Corresponsabilità

L'Istituto garantisce l'informazione alle famiglie delle attività e delle iniziative relative al tema della Cittadinanza digitale.
Ad inizio anno vengono condivisi il regolamento per la DDI e le procedure relative all'accesso a Google WorkSpace. Inoltre l'Istituto fornisce supporto ai genitori per eventuali difficoltà o problematiche riscontrate.

Gestione dell'infrastruttura e della strumentazione TIC della scuola

Strategie della scuola per garantire la sicurezza delle TIC

In tutti i plessi sono in funzione laboratori multimediali, dotati di computer fissi collegati.
Le aule sono dotate in genere di lavagna interattiva multimediale (LIM) o di un monitor interattivo e pc.
Presso la scuola secondaria di primo grado, oltre al laboratorio multimediale e alle LIM in ogni aula, sono presenti:

- un'aula magna con l'installazione di un sistema di videoconferenza.

I pc delle scuole dell'Istituto sono dotati di antivirus, monitorati e aggiornati dal tecnico dell'Istituto. Tutti i computer hanno un accesso con una password sia per gli strumenti di amministrazione, sia per l'accesso per i docenti che per gli studenti.

Strumenti di comunicazione online

Email e registro elettronico
L'Istituto utilizza due domini: @scuole.provincia.tn.it sia e @icvillalagarina.it.
Per l'invio di circolari, convocazioni e comunicazioni da parte della Segreteria si utilizza il dominio @scuole.provincia.tn.it.
Per la condivisione di materiale didattico tra docenti e docenti si utilizza il dominio @icvillalagarina.it.
I genitori con la mail del figlio/a possono contattare gli insegnanti nella mail con dominio @icvillalagarina.it.
Per le comunicazioni alle famiglie da parte della Segreteria si utilizza il dominio @icvillalagarina.it; inoltre sono caricate e condivise sul Registro Elettronico.

Sito web della scuola
L'Istituto ha un sito web, raggiungibile all'indirizzo http://www.icvillalagarina.it/.
Il Dirigente individua le modalità più adatte per la gestione delle pagine del sito e per garantire che il contenuto sia aggiornato ed appropriato, nel rispetto del contesto normativo. Il sito viene curato dal tecnico dell'Istituto.

Google WorkSpace e Classroom
La piattaforma Google WorkSpace è messa a disposizione dei docenti e degli studenti nel rispetto del regolamento della DDI.
Ad inizio anno vengono organizzati dall'Animatore Digitale dei momenti di accoglienza e alfabetizzazione digitale per i nuovi docenti e durante l'anno viene svolto uno Sportello a prenotazione per tutti i docenti.

Protezione dei dati personali
All'atto di iscrizione dei propri figli presso l'Istituto si sottoscrive un' informativa relativa al trattamento dei dati personali.
Ad inizio anno i genitori rilasciano, se lo ritengono opportuno, il consenso all'utilizzo di materiale fotografico e audiovisivo affinchè l'Istituto possa utilizzarlo sul sito web e/o altri canali istituzionali.

In caso di utilizzo di piattaforme digitali condivise o di strumenti per la creazione e gestione di classi virtuali, che richiedono l'inserimento di dati personali, viene richiesto preventivamente il consenso dei genitori.
In caso di attività di ampliamento dell'Offerta formativa organizzata da enti esterni, viene richiesto preventivamente ai genitori il consenso alle riprese audio e video e all'eventuale utilizzo per scopi didattici, informativi e divulgativi anche tramite pubblicazione su siti web.
L'accesso ai dati contenuti nel registro elettronico (ritardi, assenze, note e valutazioni) è riservato ai genitori delle Scuole Primarie e alla Secondaria di Primo Grado tramite l'invio di una password di accesso strettamente personale.

Strumentazione personale

Studenti/esse
Agli/alle alunni/e è sconsigliato portare a scuola dispositivi elettronici personali (cellulari, smartwatch) e ne è vietato l'uso non autorizzato per telefonare, messaggiare, connettersi alla rete, riprendere o registrare.
L'uso è consentito esclusivamente con specifica autorizzazione all'interno di attività didattiche espressamente programmate dai docenti.

Il divieto di utilizzo vige sia all'interno dell'edificio sia nelle zone di pertinenza (piazzale, cortile), è inoltre esteso alle attività didattiche che si svolgono in ambiente esterno alla scuola, quali viaggi di istruzione, visite guidate, uscite formative.
Il cellulare, se tenuto in cartella, deve essere rigorosamente spento.
Qualora uno/a studente/essa utilizzi o maneggi un'apparecchiatura elettronica personale senza autorizzazione, l'insegnante avrà cura di requisirla e di consegnarla in bidelleria o segreteria per essere ritirata dei genitori. Il docente segnalerà il fatto con avviso scritto sul libretto di comunicazioni scuola–famiglia e annotazione sul registro di classe o telefonata alla famiglia.

Personale docente/Assistenti educatori
Durante le ore delle lezioni e in generale durante il servizio è consentito l'uso di dispositivi elettronici personali non per comunicazioni personali, ma solo a scopo didattico o professionale.
Le password personali vanno custodite con cura e per nessuna ragione devono essere divulgate a chi non ha titolo per utilizzarle.
E' sconsigliato l'utilizzo di dispositivi di archiviazione esterna di proprietà personale, quali chiavette usb, dischi fissi portatili.

Personale ATA
Le password personali vanno custodite con cura e per nessuna ragione devono essere divulgate a chi non ha titolo per utilizzarle.
E' sconsigliato l'utilizzo di dispositivi di archiviazione esterna di proprietà personale, quali chiavette usb, dischi fissi portatili.

Situazione sicurezza

Per quanto riguarda le protezioni informatiche l'Istituto è dotato di:

- accesso alla rete di dominio garantita da nome utente e password personale;
- un firewall a protezione della rete di Istituto che verifica il traffico destinato o proveniente da reti esterne (Internet);
- una connessione Internet filtrata da proxy, uno per gli/le alunni/e ed uno per i docenti con un DNS esterno;
- un dispositivo di backup dei dati introdotti che provvede ad effettuare il salvataggio giornaliero;
- protezione antivirus sui computer configurati con il sistema operativo Windows;

L'uso di PC e Internet per gli/le alunni/e è finalizzato solo a scopi didattici ed effettuato sotto la supervisione dei docenti, in particolare:

- gli/le alunni/e della scuola primaria possono accedere ad una cartella di classe mentre i ragazzi/e della scuola secondaria ad una cartella personale; per tutti sono predisposte restrizioni sulle impostazioni. La password di accesso è a loro esclusiva conoscenza, non è comunicata al docente;
- gli/le alunni/e della primaria hanno accesso ad Internet solo se attivato dal docente; gli/le alunni/e della secondaria di primo grado hanno l'accesso a Internet sempre attivo. E´ stato escluso l'accesso ai social e altri siti con contenuti non utili ai fini didattici (filtro per argomento).

Tutti gli utenti devono usare Internet in modo responsabile proteggendo la sicurezza della propria password e segnalando tempestivamente ai responsabili della scuola eventuali disguidi, malfunzionamenti o utilizzi impropri da parte di altri.

Sono previste sanzioni per il danneggiamento del macchinario (vedi Regolamento di disciplina alunne/i).

Accertamento dei rischi e valutazione dei contenuti di Internet

La scuola adotta tutte le precauzioni necessarie per garantire agli/alle studenti/esse l'accesso a materiale appropriato, anche se non è possibile evitare in assoluto che gli/le studenti/esse trovino materiale indesiderato navigando su un computer della scuola. La scuola non può farsi carico della responsabilità per il materiale trovato su Internet o per eventuali conseguenze causate dall'accesso ad Internet.
Gli/Le studenti/esse devono essere pienamente coscienti dei rischi a cui si espongono quando sono in rete. Devono essere educati a riconoscere ed a evitare gli aspetti negativi di Internet come la pornografia, la violenza, il razzismo e lo sfruttamento dei minori. Agli/Alle studenti/esse non dovrebbe essere sottoposto materiale di questo tipo e se ne venissero a contatto dovrebbero sempre riferire l'indirizzo Internet (URL) all'insegnante o all'animatore digitale.

Prevenzione, rilevazione e gestione dei casi

Prevenzione

Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet e il coinvolgimento della comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online.
La scuola mette in atto interventi tesi a far conoscere e sensibilizzare gli/le alunni/e verso un uso responsabile e consapevole della rete, al fine di assicurare loro il rispetto del diritto ad essere tutelati da abusi e violenze da un lato e, allo stesso tempo, suscitare atteggiamenti di rispetto nei confronti degli altri utenti.
La scuola potrà avvalersi della collaborazione di esperti e associazioni per realizzare incontri rivolti agli/alle alunni/e e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica.

Il nostro Istituto inizia a **sensibilizzare** gli alunni a partire dalle classi quinte della Scuola Primaria, per proseguire durante tutti i tre anni della Scuola Secondaria di Primo Grado.

L'obiettivo è di informare ed educare alla consapevolezza ed alla riflessione su tematiche quali:

- uso e abuso di internet;
- consapevolezza dei rischi della rete;
- conoscenza delle modalità da adottare per la propria e altrui privacy;
- conoscenza delle regole e norme etiche da adottare quando si naviga in rete, quando si pubblica e quando si condivide.

La **prevenzione** avviene attraverso azioni che sviluppano le competenze digitali, previste dal curricolo.
Il nostro Istituto prevede quanto segue:

- propone incontri e corsi incentrati sul benessere online;
- organizza incontri per gli studenti e genitori con la Polizia Postale;
- dispone di uno Sportello d'Ascolto con lo psicologo della scuola, aperto per studenti, docenti e famiglie;

- forma il personale scolastico su queste tematiche;
- educa gli alunni ad un uso corretto degli strumenti digitali;
- informa e sensibilizza gli studenti circa i rischi e le conseguenze derivanti da comportamenti non adeguati e che si possono configurare come reati;
- condivide e si confronta con le famiglie sulle strategie più efficaci per sostenere i loro figli in caso di eventuale fragilità e per eventuali azioni da intraprendere nel caso siano state rilevate delle problematiche in questi ambiti.
- previene e contrasta bullismo e cyberbullismo

Fenomeni da tenere sotto osservazione e prevenire

Con le azioni programmate e realizzate annualmente, il nostro Istituto si propone di contrastare i principali fenomeni legati all'uso scorretto della Rete:

- **Hate Speech:** il fenomeno di "incitamento all'odio" indica discorsi (post, immagini, commenti etc..) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenenti a un gruppo o categoria) e che rischiano di creare reazioni violente e a catena. Questo fenomeno è sempre più diffuso ed è estremamente importante affrontarlo anche in campo educativo e scolastico.
- **Dipendenza da internet e gioco online:** la dipendenza da internet fa riferimento all'uso eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/ dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.
- **Sexting:** il termine indica un fenomeno molto frequente tra i giovanissimi che consiste nello scambio di contenuti mediali sessualmente espliciti; lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i soggetti delle immagini, delle foto e dei video.
- **Adescamento online (grooming):** si tratta di una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre bambini o adolescenti a superare le resistenze emotive e a instaurare una relazione intima e/o sessualizzata. I luoghi più frequenti in cui si sviluppa questa dinamica sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di messanging (whatsapp, telegram etc..) i siti e le app di teen dating (siti di incontro per adolescenti). **In Italia l'adescamento si configura come reato dal 2012**.
- **Pedopornografia:** la pedopornografia è un reato che consiste nel produrre, divulgare e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e e ragazzi/e coincolti/e in comportamenti sessualmente espliciti, concrete o simulate o qualsiasi rappresentazione degli organi sessuali ai fini soprattutto sessuali. Il reato di "pedopornografia minorile virtuale" è stabilito dalla legge n.38 del 6 febbraio 2006.

L'Istituto si impegna a sensibilizzare su questi temi docenti, personale scolastici, alunni e famiglie.

Possibili infrazioni

Sono da segnalare da parte di docenti, personale ATA, alunni/e, genitori:

- l'utilizzo di dispositivi in modalità e orari non consentiti;

- l’utilizzo dei dispositivi senza autorizzazione e/o sorveglianza di personale educativo;
- l’utilizzo in modo improprio o senza autorizzazione di dati sensibili o riservati (foto, immagini, video personali, informazioni private, ecc.);
- la pubblicazione di contenuti lesivi dell’immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un’istigazione alla violenza, ecc.);
- la pubblicazione di contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale;
- la navigazione su siti non idonei e/o vietati;
- la navigazione su siti che inducano a comportamenti lesivi della persona;
- il passaggio di materiali non idonei sui pc della scuola.

Rilevazione

La rilevazione dei casi è compito dell'intera comunità educante. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni o illegali, diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.
Gli/Le alunni/e vanno incoraggiati a riportare qualsiasi situazione problematica agli adulti di riferimento anche in forma anonima.
Chi segnala ha diritto alla riservatezza: la sua identità non dovrà essere resa pubblica specialmente nel caso si tratti di minore. In nessun caso dovrà subire conseguenze negative in seguito alla sua segnalazione.
Le procedure sono comunicate e condivise con l’intera comunità scolastica.

Gestione dei casi

Tutte le infrazioni andranno tempestivamente segnalate al Dirigente scolastico che, a seconda della gravità, convocherà l’animatore digitale e il consiglio di classe per valutare le possibili azioni da intraprendere; qualora le infrazioni si configurino come vero e proprio reato, avvierà gli adempimenti del caso.

La gestione dei casi rilevati va differenziata a seconda della loro gravità:

- nei casi meno problematici il consiglio di classe può gestire la situazione autonomamente coinvolgendo i genitori degli interessati e la classe in attività di riflessione sul tema emerso;
- nei casi più complessi il Dirigente, il consiglio di classe e l’animatore digitale scolastico valutano le azioni da intraprendere, comprese eventuali segnalazioni alle autorità competenti.

I genitori degli/delle alunni/e coinvolti/e vengono informati immediatamente dei comportamenti segnalati.

Come segnalare

Il personale della scuola, anche con l’ausilio del personale tecnico e dell’animatore digitale, dovrà provvedere a conservare le eventuali tracce di una navigazione non consentita su Internet o del passaggio di materiali inidonei sui pc della scuola.

Tali prove saranno utili anche ad informare la famiglia dell'alunno/a vittima di abuso, il Dirigente scolastico e, ove si configurino reati, la Polizia Postale.
In assenza di prove oggettive si raccoglieranno testimonianze sui fatti da riferire al Dirigente scolastico ed, eventualmente, alla Polizia Postale.

Casi particolari

Cyberbullismo
Qualora ci si trovi di fronte ad un caso di cyberbullismo si dovrà:

- informare i genitori degli/delle alunni/e coinvolti/e;
- coinvolgere l'animatore digitale e gli operatori scolastici su quanto sta accadendo;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online;
- tenere traccia di quanto successo e delle azioni intraprese.

Azione	Persone coinvolte	Attività
1. Segnalazione	Genitori Insegnanti Alunni/e Personale ATA	Segnalare comportamenti non adeguati e/o episodi di bullismo/cyber bullismo.
2. Raccolta informazioni	Dirigente Animatore digitale Docenti Consiglio di classe Personale ATA	Raccogliere, verificare e valutare le informazioni.
3. Interventi educativi	Dirigente Animatore digitale Docenti Consiglio di classe Alunni/e Genitori Psicologi	Incontri con gli/le alunni/e coinvolti/e. Interventi, discussione in classe. Informare e coinvolgere non solo i genitori direttamente coinvolti, ma anche i rappresentanti di classe. Responsabilizzare gli/le alunni/e coinvolti/e. Ristabilire regole di comportamento in classe. Lettera di scuse da parte del bullo; Scuse in un incontro con la vittima con la mediazione di un docente di classe. Counselling.
4. Interventi disciplinari	Dirigente Docenti Consiglio di classe Alunni/e Genitori	Si rimanda al Regolamento di disciplina alunne/alunni.

5. Valutazione	Dirigente Docenti Consiglio di classe	Dopo gli interventi educativi e disciplinari: se il problema è risolto: attenzione e osservazione costante; se la situazione continua: proseguire con gli interventi.

Sexting:
Qualora ci si trovi di fronte a un caso di sexting si dovrà:

- coinvolgere la classe e confrontarsi con esperti, facendo appello, per esempio, ad eventuali sportelli d'ascolto dell'Istituto per capire come approfondire e affrontare il fenomeno;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti riconducibili al sexting;
- documentarsi opportunamente sulle norme giuridiche che regolano i comportamenti e le condotte sessuali in Italia;
- intraprendere con la classe attività mirate a riflettere sulla fiducia che ciascuno ripone negli altri e sul fenomeno del sexting, approfondendo casi e testimonianze.

Adescamento online:
Riconosciuta una situazione di adescamento online è bene:

- approfondire la situazione coinvolgendo la classe e l'intera comunità scolastica;
- avviare dei percorsi di riflessione in classe sul concetto di fiducia;
- farsi affiancare da esperti, ricorrendo anche ad eventuali sportelli d'ascolto per offrire ai minori, qualora lo desiderino, il supporto necessario.

Strumenti a disposizione di studenti e studentesse

Per aiutare gli alunni a segnalare eventuali situazioni problematiche, la scuola può prevedere alcuni strumenti per la segnalazione ad hoc messi a loro disposizione:

- eventuale mail docente coordinatore;
- scatola/ box per la raccolta anonima di segnalazioni;
- sportello psicologo d'Istituto;

Glossario

La seguente tabella contiene le definizioni dei principali rischi connessi alla navigazione sul web:

Adescamento Online o Grooming	Il grooming (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano gli strumenti (chat, SMS, social network, ecc) messi a disposizione dalla Rete (ma anche dai cellulari) per entrare in contatto con loro. Il grooming definisce il percorso attraverso il quale gradualmente l'adulto instaura una relazione - che deve connotarsi come sessualizzata - con il/la bambino/a o adolescente.
Cyberbullismo	Il cyberbullismo (detto anche "bullismo elettronico") è una forma di prepotenza virtuale attuata attraverso l'uso di Internet e delle tecnologie digitali. Come il bullismo tradizionale è una forma di prevaricazione e di oppressione reiterata nel tempo, perpetrata da una persona o da un gruppo di persone più potenti nei confronti di un'altra percepita come più debole. Tale specifica forma di bullismo ha caratteristiche peculiari: • è pervasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo; • è un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo; • spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate. Il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamenti se non viene aiutato con riflessioni guidate.
Flaming	Litigi on line nei quali si fa uso di un linguaggio violento e volgare.
Harassment	Molestie attuate attraverso l'invio ripetuto di linguaggi offensivi.
Cyberstalking	Invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità.
Denigrazione	Pubblicazione di pettegolezzi e commenti crudeli, calunniosi e denigratori all'interno di comunità virtuali, quali newsgroup, blog, forum di discussione, messaggistica immediata, siti Internet.
Outing estorto	Registrazione delle confidenze raccolte all'interno di un ambiente privato creando un clima di fiducia e poi inserite integralmente in un blog.

Impersonificazione	Insinuazione all'interno dell'account di un'altra persona con l'obiettivo di inviare dal medesimo messaggi ingiuriosi che screditino la vittima.
Esclusione	Estromissione intenzionale dall'attività on line.
Sexting	Invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale.
Sextortion	Pratica utilizzata dai cyber criminali per estorcere denaro, la vittima viene convinta a inviare foto e/o video osé e poi le si chiede un riscatto per non pubblicarle.
Violazione della Privacy	La privacy è il diritto alla riservatezza della propria vita privata e al controllo dei propri dati personali. Il concetto di privacy è correlato a quello di dato personale, che rappresenta ogni informazione che sia relativa all'identità della persona, attraverso la quale è identificata o identificabile.
Pornografia	Recenti ricerche hanno sottolineato come la maggior parte degli adolescenti reperiscono in Rete informazioni inerenti la sessualità, col rischio, spesso effettivo, del diffondersi di informazioni scorrette e/o l'avvalorarsi di falsi miti.
Pedopornografia	Foto o video di natura sessuale che ritraggono persone minorenni.
Gioco d'azzardo o Gambling	Giocare d'azzardo significa "puntare o scommettere una data somma di denaro, o oggetto di valore, sull'esito di un gioco che può implicare la dimostrazione di determinate abilità o basarsi sul caso".
Dipendenza da Internet	Coloro che ne soffrono sono spesso inconsapevoli ma, lontani dalla rete, manifestano presto insofferenza, irascibilità e altri sintomi di disagio.
Videogiochi online	Alcuni rischi associati possono essere ad esempio: contatti impropri con adulti, contenuti violenti e/o inadeguati; acquisti incontrollati, ecc.
Esposizione a contenuti dannosi o inadeguati	Es. contenuti razzisti, che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, ecc.
Dipendenza da shopping online	Es. acquisti incontrollati, uso della carta di credito dei genitori a loro insaputa, ecc.

Riferimenti normativi

Il bullismo e il cyberbullismo devono essere conosciuti e combattuti da tutti in tutte le forme, così come previsto da numerosi atti normativi fra cui ricordiamo i seguenti::

- artt. 3- 33- 34 della Costituzione Italiana;
- artt. 581-582-594-595-610-612-635 del Codice Penale;
- artt. 2043-2047-2048 Codice Civile;
- D.P.R. 249/98 e 235/2007: *"Regolamento recante lo Statuto delle studentesse e degli studenti della scuola secondaria*";
- Direttiva MIUR n.16 del 5 febbraio 2007 "*Linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo*";
- direttiva MPI n. 30 del 15 marzo 2007 "*Linee di indirizzo ed indicazioni in materia di utilizzo di 'telefoni cellulari' e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità dei genitori e dei docenti"* e successive modifiche/integrazioni;
- direttiva MPI n. 104 del 30 novembre 2007 "*Linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all'utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali";*
- linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo (MIUR Aprile 2015);
- Legge n. 71 del 29 maggio 2017 "*Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyber bullismo".*
- Aggiornamento delle linee di orientamento per la prevenzione e il contrasto del cyber bullismo, MIUR, Ottobre 2017

Allegato 1

Netiquette

Fra gli utenti dei servizi telematici di rete si è sviluppata, nel corso del tempo, una serie di tradizioni e di norme di buon senso che costituiscono la "Netiquette" che si potrebbe tradurre in "Galateo (Etiquette) della rete (Net)": il Galateo della rete.

Ecco alcune regole che TUTTI GLI UTENTI(studenti- famiglie- personale) dovrebbero seguire:

1.Non essere offensivi
Il testo è l'unico mezzo attraverso il quale comunicare con gli altri in rete. Il tono della voce, l'espressione del viso, non possono essere di aiuto per far comprendere all'altro il senso del discorso. Il rischio di essere fraintesi è altissimo.
Tieni sempre presente questa regola quando scrivi e usi gli emoticons (emotional icons) per ribadire il tono del messaggio:  scherzoso;  allegro;  triste e cosi via.

2.Scegliere l'ambiente adatto a se stessi
Ogni chat, mailing list, newsgroup, forum ha delle caratteristiche specifiche e non si può trovare sempre argomenti adatti a noi o di nostro interesse.
Scegli la community che si avvicina di più alle tue esigenze, ma soprattutto quella dove ti senti più a tuo agio, anche grazie al controllo del moderatore.

3.Seguire regole di comportamento analoghe alle proprie regole di vita
L'identità digitale dovrebbe corrispondere all'identità personale che ognuno agisce nella vita reale.
Se nella vita reale non ruberesti mai un prodotto, non scaricare software abusivamente o illegalmente dalla Rete, non usare o copiare software che non hai pagato.

4.Scegliere di essere paziente e comprensivi
Quando s'invia un messaggio non bisogna pretendere subito la risposta. Chi comunica con noi può non essere interessato all'argomento che proponiamo oppure può non avere il tempo di rispondere.
Dà il tempo di rispondere… e rifletti anche tu prima di rispondere.

5.Presentarsi con cura
In rete si hanno solo le parole per farsi conoscere. Bisogna usarle con cura, scegliendo quelle di cui si è veramente convinti, solo così daremo a chi comunica con noi l'impressione di come siamo veramente.
Prenditi il tempo per presentarti quale sei veramente.

6.Essere prudente
In rete si possono trovare le persone più diverse e non sempre si presentano per ciò che sono realmente. È indispensabile agire con prudenza.
Non credere a tutto quello che viene detto. Non accettare senza riflettere di fare ciò che ti viene richiesto in rete o di incontrare qualcuno che hai appena conosciuto.

7.Rispettare la privacy
Non vanno diffuse in rete informazioni riguardanti la vita e le abitudini altrui, così come è indispensabile proteggere i propri dati personali.
Non diffondere informazioni, immagini, dati che riguardano i tuoi amici e limita allo stretto indispensabile anche la condivisione di ciò che riguarda la tua vita e la tua famiglia.

8.Scegliere toni moderati
Se si esprime il parere in maniera pacata è meno probabile che le parole usate possano provocare reazioni dure da chi comunica con noi. Basta poco per infiammare una discussione e serve invece molto tempo per tornare ad un dialogo tranquillo.
Scegli con cura le parole a sostegno delle tue idee e non alimentare l'odio on line.

9.Non urlare
Scrivere in maiuscolo su Internet equivale ad urlare: è uno strumento a disposizione per enfatizzare quello che stai dicendo. Fai attenzione a non abusarne!

10.Trascurare gli errori degli altri
Il desiderio di rispondere velocemente porta a errori di digitazione, di grammatica o di sintassi ma l'importante è che il messaggio sia comprensibile.
Sii comprensivo con gli altri, nella comunicazione veloce potresti sbagliare anche tu!

11.Utilizzare la rete per ampliare le conoscenze
Internet è una sterminata enciclopedia a portata di mouse ed offre anche la possibilità di leggere le opinioni degli altri su qualsiasi argomento. Si possono trovare informazioni specialistiche, il materiale per una ricerca scolastica o anche solo confrontare la propria opinione.
Usa la rete, non farti usare dalla rete!

12.Non abusare delle proprie conoscenze
Non si dovrebbero usare le proprie competenze digitali per entrare nel mondo altrui, per violare siti, profili o per venire in possesso di contenuti.
Evita di usare le tue competenze per danneggiare gli altri.

13.Dimenticare le differenze
La rete è un mondo nel quale l'unico strumento è la tastiera, l'unico oggetto visibile il monitor. Non ha nessuna importanza il colore della tua pelle, la tua religione.
Concentrati sul contenuto dei massaggi, apprezza quanto viene scritto.

Allegato 2

SCUOLA SECONDARIA DI PRIMO GRADO

REGOLAMENTO SULL'UTILIZZO DELLE APPARECCHIATURE E DEI LABORATORI INFORMATICI E DELLE POSTAZIONI MULTIMEDIALI E RETI PRESENTI NELLA SCUOLA

- L'utilizzo dei personal computer della scuola, del laboratorio di informatica, della biblioteca e dell'aula magna è destinato all'attività didattica e gli/le studenti/esse potranno farne uso solo se accompagnati dall'insegnante.
- Ogni spostamento di materiali o parti di esse (es. mouse, tastiere, monitor, cuffie, ecc.) da un locale all'altro deve essere autorizzato dall'assistente di laboratorio o dai responsabili di laboratorio.
- Non è consentito l'uso di prodotti software che non siano stati regolarmente acquistati dalla scuola e per i quali non sia stata rilasciata licenza d'uso, a meno che non siano prodotti freeware. I docenti e gli/le studenti/esse non possono installare software sui PC della scuola; ma possono richiederne l'installazione all'assistente di laboratorio.
- Non è consentito l'uso delle attrezzature dell'aula per la riproduzione di materiale coperto da copyright. Chiunque venisse a conoscenza di tali operazioni è tenuto a darne comunicazione al responsabile di laboratorio o all'assistente di laboratorio.
- L'uso di Internet deve essere di valenza didattica. E' quindi del tutto sconsigliato senza un'adeguata vigilanza e previa informazione all'assistente di laboratorio, utilizzare servizi "World Wide web" (e-mail, forum, chat, blog, file sharing, e-commerce, ecc.) per scopi non legati a studio o attività didattica e professionale delle/i docenti.
- Eventuali guasti, malfunzionamenti o sostituzioni di materiale di consumo vanno segnalati all'insegnante referente dell'aula, mediante la compilazione dell'apposito modulo relativo ad ogni postazione.

E´ vietato:

- Utilizzare CD Rom, DVD Rom, chiavette USB o altri supporti di memoria personali senza averli preventivamente sottoposti al controllo antivirus prima di ogni utilizzo.
- Modificare le configurazioni di sistema delle macchine.

E´ vietato e perseguibile:

- Utilizzare programmi atti a violare la sicurezza dei sistemi locali e remoti.
- Inserire password aggiuntive per bloccare o disabilitare qualsiasi funzione o documento; tutti i documenti dovranno essere in chiaro, non protetti e non criptati."
- **Inviare mail o inserire comunicazioni/commenti sul REL/CLASSROOM nei giorni di sabato/domenica/festivi e dal lunedì al venerdì dalle ore 20.00 alle ore 7.00 (silenzio digitale). Si consiglia di usare la programmazione di invio.**

Allegato 3

SCUOLA PRIMARIA

REGOLAMENTO SULL'UTILIZZO DELLE APPARECCHIATURE E DEI LABORATORI INFORMATICI E DELLE POSTAZIONI MULTIMEDIALI E RETI PRESENTI NELLA SCUOLA

- L'utilizzo dei personal computer della scuola e dei laboratori informatici è destinato all'attività didattica e gli/le alunni/e potranno farne uso solo se accompagnati dall'insegnante.
- Ogni spostamento di materiali, macchine o parti di esse (es. mouse, tastiere, monitor, stampanti, ecc.) da un locale all'altro deve essere autorizzato dall'assistente di laboratorio o dai responsabili di laboratorio.
- Non è consentito l'uso di prodotti software che non siano stati regolarmente acquistati dalla scuola e per i quali non sia stata rilasciata licenza d'uso, a meno che non siano prodotti freeware. I docenti e gli/le studenti/esse non possono installare software sui PC della scuola; ma possono richiederne l'installazione all'assistente di laboratorio.
- Non è consentito l'uso delle attrezzature dell'aula per la riproduzione di materiale coperto da copyright. Chiunque venisse a conoscenza di tali operazioni è tenuto a darne comunicazione al responsabile di laboratorio o all'assistente di laboratorio.
- L’accesso ad Internet da parte degli/delle alunni/e deve essere autorizzato dal docente e per scopi didattici.
- Eventuali guasti, malfunzionamenti o sostituzioni di materiale di consumo vanno segnalati all’insegnante referente dell’aula, mediante la compilazione dell’apposito modulo relativo ad ogni postazione.

E´ vietato:

- Utilizzare CD Rom, DVD Rom, chiavette USB o altri supporti di memoria personali senza averli preventivamente sottoposti al controllo antivirus prima di ogni utilizzo.
- Modificare le configurazioni di sistema delle macchine.
- **Inviare mail o inserire comunicazioni/commenti sul REL/CLASSROOM nei giorni di sabato/domenica/festivi e dal lunedì al venerdì dalle ore 20.00 alle ore 7.00 (silenzio digitale). Si consiglia di usare la programmazione di invio.**

- **.**

E´ vietato e perseguibile:

- Utilizzare programmi atti a violare la sicurezza dei sistemi locali e remoti.
- Inserire password aggiuntive per bloccare o disabilitare qualsiasi funzione o documento; tutti i documenti dovranno essere in chiaro, non protetti e non criptati."