



ISTITUTO COMPRENSIVO VIA MARSALA
Via Marsala 13 – 27058 Voghera (PV) Tel. 0383- 41371 - Fax 0383 41598- C.F. 9503277182
Email: PVIC826009@istruzione.it – PEC: PVIC826009@PEC.ISTRUZIONE.IT
Sito web: www.icviamarsalavoghera.gov.it – COD. UNIVOCO UFFICIO UF1EN

E-Policy

1-INTRODUZIONE

Con il presente documento l'IC di via Marsala si dota di una *e-policy*, ovvero di un sistema ordinato di informazioni, procedure e regole relative all'uso consapevole e sicuro di internet e delle tecnologie digitali all'interno della scuola.

Attenzione particolare è dedicata alla prevenzione, rilevazione e presa in carico di situazioni di pericolo per gli alunni, derivanti da un uso non consapevole o scorretto di internet (cyberbullismo, sexting, pedopornografia, grooming, gioco d'azzardo...).

2-RUOLI E RESPONSABILITÀ DEGLI ATTORI DELLA COMUNITÀ SCOLASTICA

Il Dirigente Scolastico

- Segue le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo di internet o dei dispositivi digitali;
- predispone e garantisce l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- redige un piano di formazione affinché tutti gli insegnanti possano svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC);
- garantisce la sicurezza on-line dei membri della comunità scolastica.

I Collaboratori del Dirigente Scolastico

- Svolgono un ruolo di supporto al Dirigente Scolastico nella pianificazione ed implementazione della *E-Policy* d'Istituto.

Il Referente d'Istituto per la prevenzione ed il contrasto del cyberbullismo

- Nel rispetto dell'Art. 4 comma 3, della Legge 71/2017, il Referente d'Istituto per la prevenzione ed il contrasto del cyberbullismo ha il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo, anche avvalendosi

della collaborazione delle Forze di Polizia, nonché delle associazioni e dei centri di aggregazione giovanile presenti sul territorio.

L'animatore digitale

- Realizza corsi interni all'Istituto e promuove tutte le iniziative della rete di scuole, relativi alla sicurezza digitale e all'utilizzo delle TIC;
- fornisce consulenza e informazioni al personale scolastico in relazione alla navigazione in rete, ai rischi *on-line* e alla loro gestione;
- monitora l'insorgere di problematiche in rapporto all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- revisiona periodicamente le politiche sulla *e-safety*, individua soluzioni metodologiche e tecnologiche innovative e sostenibili, da diffondere a scuola;
- segnala al DSGA le esigenze relative all'acquisto di strumenti e dispositivi o all'intervento di personale tecnico;
- partecipa all'ideazione e alla progettazione di attività e percorsi attinenti la scuola digitale.

II DSGA

- assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici e l'acquisto di strumenti e dispositivi necessari per garantire che l'infrastruttura tecnica della scuola sia funzionante e sicura.

I docenti

- Conoscono la politica di sicurezza adottata dalla scuola e rispettano il regolamento;
- si aggiornano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet;
- segnalano all'Animatore Digitale qualsiasi esigenza di formazione o di carattere tecnico-organizzativo;
- integrano nel curriculum di studio e nelle attività didattiche ed educative delle classi le regole per un uso corretto e sicuro delle TIC;
- mettono in atto procedure affinché gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- garantiscono che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale;
- assicurano la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllano che l'uso dei dispositivi digitali avvenga nel rispetto degli usi e dei tempi previsti dalla regolamentazione d'Istituto;
- nelle lezioni in cui è previsto l'uso di internet, guidano gli alunni nella scelta e nell'utilizzo di materiali e contenuti idonei;
- utilizzano le misure previste dalla scuola per prevenire le diverse tipologie di rischio ed attuare le specifiche procedure per la gestione delle problematiche,
- segnalano al D.S. qualsiasi abuso rilevato a scuola;

- comunicano ai genitori bisogni e difficoltà o condotte non adeguate degli alunni, rilevati a scuola e connessi all'utilizzo delle TIC, al fine di concordare linee condivise di supporto.

I genitori

- conoscono i regolamenti e le linee adottati dalla scuola e ne sostengono il rispetto da parte dei propri figli;
- sorvegliano l'utilizzo di internet e delle tecnologie digitali da parte dei propri figli a casa nello svolgimento dei compiti;
- concordano e condividono con i docenti regole, strategie e comportamenti volti a garantire la maggiore sicurezza e consapevolezza possibili nell'uso di internet e delle nuove tecnologie da parte degli alunni.

3 - CONDIVISIONE DELLA E-POLICY

- A seguito di delibera degli organi collegiali, il presente documento sarà condiviso con tutto il personale in servizio e con la componente genitori mediante pubblicazione su sito web della scuola.
- Durante le occasioni di incontro scuola-famiglia verranno illustrate ai genitori le caratteristiche della *E-Policy* di istituto ed il regolamento interno, favorendo un clima di collaborazione e coerenza negli interventi educativi.
- La scuola avrà cura di fornire un'adeguata formazione del personale docente rispetto all'uso sicuro di internet.
- Tutti gli alunni saranno informati rispetto alle regole sull'utilizzo di internet e di ogni dispositivo digitale all'interno della scuola, tenendo conto delle rispettive fasce d'età.
- La scuola creerà occasioni curricolari ed extracurricolari per educare gli alunni ed informare le famiglie rispetto ai rischi su internet a cui i minori risultano più esposti.
- La scuola si impegna alla trasparenza nei confronti dei genitori rispetto alle norme e alle disposizioni che riguardano l'uso di internet e dispositivi digitali a scuola.

4 - GESTIONE DELLE INFRAZIONI DELLA E-POLICY

Laddove il personale docente ed educativo ravvisi da parte di uno o più alunni della classe o di un plesso elementi che indicano una particolare esposizione a fattori di rischio o una condotta in conclamata antitesi con le linee guida di questo documento, verranno attuate le seguenti misure:

- 1) tempestiva segnalazione al Dirigente Scolastico;
- 2) segnalazione al coordinatore di classe e condivisione all'interno del consiglio di classe per la scuola secondaria di 1° grado; condivisione all'interno *del team* per le scuole dell'infanzia e primaria;
- 3) attuazione di interventi correttivi e sanzioni laddove opportuno;
- 4) predisposizione e attuazione di interventi informativi ed educativi *ad hoc*, da parte dei docenti e/o di esperti esterni.

Principali infrazioni a carico degli alunni:

- utilizzo a scuola del cellulare o di dispositivi mobili personali senza l'esplicita e motivata autorizzazione da parte del docente presente in quel momento;
- utilizzo della rete internet scolastica per scopi diversi da quanto indicato dai docenti;
- condivisione di dati sensibili, foto e informazioni intime, *sexting*;
- uso della rete e dei dispositivi mobili per deridere, screditare o ledere il benessere psicologico e sociale di altre persone;
- condivisione di materiale violento, pornografico, che incoraggia comportamenti pericolosi o lesivi per sé o per altri;
- condivisione di materiale che incoraggia odio e comportamenti discriminatori verso specifiche categorie di persone (in base a sesso, razza, identità di genere, orientamento sessuale, credo religioso, provenienza geografica, disabilità, aspetto fisico...) o in generale verso terzi;

Gli interventi correttivi e le sanzioni previsti sono correlati alla gravità o reiterazione del comportamento, all'età e al livello di sviluppo dell'alunno, e comprendono i seguenti provvedimenti disciplinari:

- richiamo verbale;
- sospensione dell'attività e/o ritiro del dispositivo mobile;
- richiamo scritto con annotazione su diaro e/o libretto e/o registro elettronico;
- sospensione;
- convocazione e colloquio con i genitori da parte dell'insegnante o del Dirigente Scolastico

Sono, altresì, considerati elementi di attivazione di specifiche procedure i seguenti scenari:

- ragionevole sospetto che uno o più alunni siano vittima di cyberbullismo, adescamento da parte di adulti malintenzionati o pedofili;
- dipendenza psicologica da meccanismi diffusi via web che incitano comportamenti pericolosi o autolesivi (*challenge*, catene...).

5 - INTERVENTI DI SUPPORTO, SOSTEGNO E INFORMAZIONE:

- colloquio a tu per tu tra il docente (o se necessario il Dirigente Scolastico) e l'alunno che vive una situazione, al fine di far percepire la presenza e il sostegno da parte degli adulti responsabili e di conoscere più dettagliatamente i confini del problema;
- colloquio tra il docente (o se necessario il Dirigente Scolastico) e i genitori dell'alunno coinvolto in una situazione-problema, al fine di elaborare strategie condivise di supporto all'alunno;
- orientamento dell'alunno verso lo sportello psicologico della scuola;
- interventi generalizzati rivolti alla classe o a gruppi di classi al fine di garantire una comprensione e consapevolezza del fenomeno individuato e delle corrette pratiche (realizzati da parte degli insegnanti o di esperti esterni individuati dalla scuola);

- progetti ad hoc all'interno della classe o di gruppi di classi per esplicitare le modalità relazionali all'interno del gruppo ed apprendere come costruire e gestire relazioni in modo positivo (realizzati da parte di esperti individuati dalla scuola).

6 - PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

Prevenzione

RISCHI

I rischi in cui gli allievi possono incorrere nell'utilizzo scorretto delle TIC, eludendo la sorveglianza degli insegnanti, sono molteplici e derivano da:

- telefoni cellulari e altri dispositivi portatili con accesso a internet;
- applicazioni di messaggistica e social network, che consentono la condivisione istantanea di foto e video;

I medesimi rischi potrebbero trovarsi durante l'uso del pc del laboratorio informatico a scuola e con accesso non controllato a internet.

AZIONI

Le azioni di prevenzione previste nell'utilizzo delle TIC sono le seguenti:

- informare e formare i docenti, i genitori, il personale ATA e gli studenti sui rischi che un uso non sicuro delle nuove tecnologie può favorire;
- fornire ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori (es. liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio/a figlio/a);
- non consentire l'utilizzo del cellulare personale degli alunni a scuola, in quanto per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola supervisionato dall'addetto al centralino, che prima di passare la telefonata si accerta dell'identità dell'interlocutore;
- consentire l'utilizzo del cellulare solo in casi eccezionali, ad esempio quando ci si trova fuori dal contesto scolastico durante una visita guidata e sempre sotto la supervisione di un insegnante che si accerta dell'identità dell'interlocutore;
- utilizzare filtri che non permettano la connessione a siti web per adulti centralizzando il blocco dei siti web sul server del docente.

Rilevazione

Che cosa segnalare.

Gli alunni possono mostrare segni di tristezza o di ansia o di risentimento nei confronti di compagni o di altri e riferire spontaneamente o su richiesta l'accaduto ai docenti. I fatti riferiti possono essere accaduti anche al di fuori della scuola. Talvolta confrontandosi periodicamente con gli alunni sui rischi delle comunicazioni on-line, i minori possono riferire di fatti o eventi personali o altrui che "allertano" l'insegnante.

Una "prova" di quanto riferito può essere presente nella memoria degli strumenti tecnologici utilizzati, può essere mostrata spontaneamente dall'alunno, essere presentata da un reclamo dei genitori o essere notata dall'insegnante.

Il docente è autorizzato a controllare le strumentazioni della scuola, mentre per controllare l'uso del telefono cellulare o di dispositivi personali di un alunno occorre che si rivolga al genitore.

Per gli alunni i contenuti "pericolosi" comunicati o ricevuti da altri, messi in rete o scaricati da essa, possono essere i seguenti:

- contenuti che violano la privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private, proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati ecc.);
- contenuti aggressivi o violenti (messaggi minacciosi, commenti offensivi, pettegolezzi ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o immagini pornografiche.

Le azioni di contenimento degli incidenti previste sono le seguenti:

- rimuovere immagini che violano la privacy propria o altrui, di natura sessuale o violenta, o di altra identità non desiderata tramite il service provider;
- modificare dettagli del proprio profilo qualora l'alunno venga infastidito sistemandolo su "privato", in modo che solo gli utenti autorizzati possano vederlo, oppure bloccare o ignorare alcuni mittenti cancellando anche il loro nominativo dalla lista degli amici;
- consigliare di cambiare il proprio indirizzo e-mail, contattando l'e-provider, di scaricare un'applicazione che blocchi chiamate e messaggi da numeri indesiderati o se necessario cambiare numero telefonico;
- far cancellare il materiale offensivo dal proprio telefonino facendo intervenire i genitori, conservandone una copia se necessario per poter far condurre indagini in proposito;
- contattare la polizia postale o segnalare ad essa materiale considerato offensivo o illegale e confiscare il telefonino se si tratta di materiale pedopornografico per evitare che venga ulteriormente divulgato in vari modi.

7 - COME E A CHI SEGNALARE

- Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.
- Gli insegnanti, anche con l'ausilio tecnico dell'Animatore Digitale, possono provvedere ugualmente a conservare le prove della condotta incauta, scorretta o dell'abuso-rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto.
- Qualora ci si dovesse accorgere che l'alunno, usando il computer, si sta servendo di un servizio di messaggia istantanea, l'insegnante può copiare, incollare e stampare la conversazione.
- Per eventuali collegamenti non autorizzati a *social network*, *video-hosting sites* e altri siti, l'insegnante può conservare il *link*, stampare la pagina o salvare la schermata su documento di testo.
- I messaggi *e-mail* possono essere stampati o conservati integralmente (compresa l'intestazione del mittente).

Conservare la prova è utile per far conoscere l'accaduto in base alla gravità ai genitori degli alunni, al Dirigente Scolastico e, per le condotte criminose, alla polizia.

Qualora non si disponga di prove, ma solo delle testimonianze dell'alunno, quantunque riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte sono comunque comunicate ai genitori e, per fatti rilevanti, al Dirigente Scolastico; per quelle criminose, anche alla polizia.

In particolare la segnalazione viene fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.

Per le segnalazioni di fatti rilevanti sono previsti i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto:

- annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata;
- convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;
- relazione scritta al Dirigente scolastico.

In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali.

Per i reati meno gravi la legge rimette ai genitori degli alunni la scelta di richiedere la punizione del colpevole, attraverso la querela.

Per i reati più gravi (es. pedopornografia) gli operatori scolastici hanno l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).

In particolare per i fatti criminosi, ai fini della denuncia, la relazione dev' essere redatta nel modo più accurato possibile, indicando i seguenti elementi: il fatto, il giorno dell'acquisizione del fatto, le fonti di prova già note e, per quanto possibile, le generalità, il domicilio e quant'altro di utile a identificare la persona alla quale il reato è attribuito, la persona offesa e tutti coloro che sono in grado di riferire circostanze rilevanti per la ricostruzione del fatto.

8 - GESTIONE DEI CASI

Gestione dei casi di "immaturità"

Può sembrare naturale all'alunno fornire i propri dati sui siti allestiti in modo tale da attrarre l'attenzione dei bambini, con giochi e animazioni, personaggi simpatici e divertenti, che richiedono una procedura di registrazione.

Curiosità, manifestazioni di reciproco interesse tra pari, idee e fantasie sulla sessualità sono espressione da una parte del progressivo sviluppo socio-affettivo dell'alunno e dall'altra dei molteplici messaggi espliciti che gli giungono quotidianamente attraverso i media.

I comportamenti cosiddetti "quasi aggressivi", che spesso si verificano tra coetanei, le interazioni animate o i contrasti verbali, o la presa in giro "per gioco", effettuata anche in rete, mettono alla prova la relazione con i compagni, la supremazia o la parità tra i soggetti implicati e l'alternanza e sperimentazione dei diversi ruoli.

Detti comportamenti, che finiscono per arrivare all'attenzione degli adulti, sono controllati e contenuti dai docenti attraverso i normali interventi educativi, di richiamo

al rispetto delle regole di convivenza civile e democratica, e di rispetto degli altri, per evitare che possano degenerare, diventare pericolosi per sé o per altri.

Gestione dei casi di "prepotenza" o "prevaricazione"

I comportamenti definibili "Bullismo" possono esprimersi nelle forme più varie e non sono tratteggiabili a priori; se non contestualizzandoli. Le caratteristiche che aiutano a individuarli e a distinguerli dallo scherzo, dalle intemperanze caratteriali, dai diverbi usuali fra i ragazzi sono: la costanza nel tempo e la ripetitività, l'asimmetria (disuguaglianza di forza e di potere), il disagio della/e vittima/e.

Il **bullismo** può essere definito come la ripetizione di episodi violenti (violenza psicologica, verbale, o fisica) agiti da uno o più soggetti (bullo/i) nei confronti di un "bersaglio", che avvengono nell'ambiente scolastico, nelle sue adiacenze o nel percorso per recarvicarsi (es. fermata del bus). A questi episodi assiste un pubblico di pari che può essere positivo (cerca di fermare il bullo, difende il bersaglio, chiede aiuto) o negativo (guarda ma non interviene, oppure incita il bullo, oppure riprende a sua volta la scena e la diffonde mediante foto o video).

Il **cyberbullismo** è la forma *on-line* del bullismo. Si realizza attraverso l'invio di messaggi verbali, foto e/o video tramite cellulari, *smartphones*, *pc*, *tablet* (su *social network*, siti *web*, *blog*, *e-mail*, gruppi *online*, *newsgroup*, *chat*) ed ha gli stessi obiettivi della sua forma *offline*, ovvero quelli di insultare, offendere, minacciare, diffamare e/o ferire.

In considerazione dell'età degli alunni considerati possono prefigurarsi alcune forme di interazioni che possono evolvere verso tale fenomeno. Per prevenire e affrontare il bullismo dunque i docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, coinvolgendo i genitori degli allievi.

L'elemento fondamentale per una buona riuscita dell'intervento educativo è infatti la corretta, compiuta e convinta ristrutturazione dell'ambiente sociale in cui tale fenomeno si verifica, e in particolare delle relazioni nel contesto della classe. Gli atteggiamenti degli alunni, così come quelli dei loro genitori, possono giocare un ruolo molto significativo nel ridurre la dimensione del fenomeno.

Gli interventi mirati sul gruppo classe sono gestiti in collaborazione dal *team* dei docenti della classe e d'intesa con le famiglie, ad esempio con percorsi di mediazione volti alla risoluzione del conflitto, con gruppi di discussione (*circle-time*), con rappresentazioni e attività di *role-play* sull'argomento del bullismo.

Vengono intrapresi anche i percorsi individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme.

Inoltre la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia altresì di servirsi dello sportello di ascolto psicologico gratuito convenzionato. Promuove e supporta la richiesta delle famiglie rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi comunali e all'ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).

Gestione degli "abusi sessuali"

"In generale si parla di abuso sessuale sui bambini quando un bambino viene coinvolto in un atto sessuale. Ciò è caratterizzato dal fatto che il bambino non comprende del tutto tale atto, non è informato e quindi non è in grado di acconsentire, oppure sulla base del suo livello di sviluppo non è ancora pronto per tale atto e non può dare il proprio consenso".

Lo spettro delle forme di abuso e di violenza è diventato ancora più ampio e subdolo in seguito alle possibilità offerte dai nuovi mezzi di comunicazione come internet, il cellulare o altri dispositivi tecnologici, e il loro utilizzo sempre più diffuso non fa che acuire il problema.

Internet, infatti, permette di scaricare o vendere immagini o filmati di pornografia infantile. Succede sempre più frequentemente che un adulto prenda contatto con dei bambini nei *social network* o nelle *chat* su internet, e che li metta di fronte a domande o messaggi sessuali o addirittura a immagini pornografiche. A volte l'adulto induce i bambini a spogliarsi davanti alla *webcam* oppure a inviare una fotografia che li ritrae nudi tramite internet o sul cellulare, per poi ricattarli e costringerli a non rivelare gli abusi. Spesso l'adulto finge di essere minorenne.

La denuncia all'autorità giudiziaria o agli organi di Polizia, da parte degli insegnanti o del Dirigente Scolastico, costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole.

La presa in carico di situazioni di abuso sessuale, così delicate e complesse, richiede un approccio multidisciplinare, da parte di diverse figure professionali. I versanti su cui si articola l'intervento possono essere essenzialmente tre: medico, socio-psicologico e giudiziario.

Il compito della scuola non è comunque solo quello di "segnalare", ma più ampio ed importante, soprattutto nella prevenzione dell'abuso, nonché nella ripresa della piccola vittima, in quanto ha al suo interno fattori relazionali ed educativi che possono aiutare il bambino a riprendere una crescita serena.

A tal fine la scuola lavora insieme alle altre figure professionali e alle famiglie, scambiando informazioni e condividendo progetti e prassi operative, favorendo le occasioni di confronto e di dialogo.

9 - MONITORAGGIO/AGGIORNAMENTO DELLA E-POLICY

Ogni anno si procederà al monitoraggio e all'aggiornamento della *E-Policy*.

Il monitoraggio coinvolgerà i docenti di classe, con l'obiettivo di valutare la funzionalità della *E-Policy* e l'adozione di eventuali adeguamenti, con particolare attenzione all'analisi delle problematiche concretamente emerse durante l'attività scolastica quotidiana, attraverso la somministrazione di questionari e la tabulazione dei dati emersi. L'aggiornamento della *E-Policy* sarà curato dal Dirigente Scolastico, dall'Animatore Digitale, dagli Organi Collegiali, a seconda degli aspetti considerati. La valutazione dell'andamento e la revisione del documento saranno di pertinenza del Dirigente Scolastico, con la collaborazione delle seguenti figure di sistema: Collaboratori del Dirigente Scolastico, Funzioni Strumentali, Referente d'Istituto per bullismo/cyberbullismo, Animatore Digitale.

10 - E-POLICY E DOCUMENTI-CHIAVE DELL'ISTITUTO

Il documento di *E-Policy* deve risultare coerente con le linee fondanti del PTOF, del Regolamento d'Istituto, del Patto di Corresponsabilità Scuola-Famiglia. È inoltre indispensabile una correlazione integrata con le norme riguardanti l'utilizzo dei Laboratori Informatici, l'uso di software, l'accesso a Internet.

11 - UTILIZZO LABORATORI INFORMATICI

Le attrezzature informatiche vanno utilizzate con il massimo rispetto, trattandosi di bene comune.

I Laboratori Informatici sono da destinare esclusivamente ad attività di insegnamento, funzionali all'insegnamento, e di formazione del Personale Docente/Non Docente.

Il Docente che usufruisce dei Laboratori Informatici deve annotare l'orario d'uso su apposito registro.

Gli alunni possono accedere ai Laboratori Informatici solo in presenza di un docente, che risponde del corretto uso delle dotazioni.

È vietato cancellare o alterare di propria iniziativa (senza informazione preventiva e/o accordo con i creatori dei files) files presenti sul desktop dei pc. Tale disposizione vale sia per i Docenti che per gli alunni.

A conclusione delle attività, chi utilizza i Laboratori Informatici dovrà assicurarsi che le macchine siano spente correttamente e che i locali siano in ordine.

I Laboratori Informatici non devono restare aperti se incustoditi.

I Responsabili dei Laboratori Informatici devono essere tempestivamente informati di eventuali malfunzionamenti, guasti o danni alle attrezzature. Sarà cura dei Responsabili informare la Segreteria se si rendesse necessaria un'assistenza tecnica esterna.

Ai Docenti si suggerisce di salvare regolarmente su personali dispositivi di memoria esterna i dati giacenti nei PC dei Laboratori Informatici.

I Laboratori Informatici di ogni sede dell'Istituto, ove esistenti, devono dotarsi di un Regolamento scritto collocato in posizione ben visibile all'interno dei Laboratori stessi.

Modello di Regolamento

REGOLE DA SEGUIRE NELL'AULA INFORMATICA

Nel ricordare che nell'aula informatica si trovano materiali il cui costo è molto elevato, vengono proposte le seguenti **regole** che andranno osservate categoricamente da tutti gli alunni: chi non osserverà tali regole verrà **escluso dal laboratorio** per un periodo di tempo che varierà a seconda della gravità dell'infrazione.

1. Rimanere seduti nella **postazione assegnata**, ciascuno **è responsabile** del computer assegnato. Ciò serve a risalire al responsabile di eventuali danni al sistema operativo o di visite a siti inopportuni.

2. Controllare che l'interruttore generale sia acceso quindi avviare il Pc tramite il **tasto posto sopra la scatola (case)** del computer. Il monitor è sempre acceso quindi **non intervenire mai** sui pulsanti dello stesso.

3. In caso di difficoltà **richiamare l'attenzione dell'insegnante.**
4. Non cambiare la configurazione del video, né modificare gli sfondi o le impostazioni dello schermo, né tanto meno scaricare programmi o applicazioni **senza l'autorizzazione dell'insegnante.**
5. Se nell'accendere il computer si notasse qualche anomalia, questa va **segnalata subito all'insegnante**, così facendo ci si libera della responsabilità relativa all'accaduto.
6. Nel caso in cui la postazione sia condivisa da due alunni **si deve lavorare tutti e due** alternandosi ai comandi del Pc in modo che tutti acquisiscano le necessarie competenze.
7. Tutti i lavori svolti vanno salvati in una apposita cartella creata all'interno del seguente percorso:

Documenti / 1C Cognome1-Cognome 2

esempio: 1A Montagna-Brambilla

8. Al termine della lezione ascoltare le indicazioni dell'insegnante circa lo spegnimento dei computer. In ogni caso **sistemare sempre le sedie in ordine** sotto le postazioni e attorno al tavolo.

Il Referente del Laboratorio di Informatica

Utilizzo dei software

I *software* installati sono ad esclusivo uso didattico.

È vietato usare *software* non conformi alle leggi vigenti.

Occorre avvisare preventivamente i Responsabili dei laboratori Informatici circa la volontà di procedere ad una qualsiasi forma di installazione sui PC.

Accesso a Internet

Gli alunni hanno possibilità di accedere ad internet solo in presenza di Docenti accompagnatori e per uso esclusivamente didattico. La navigazione su internet è consentita al Personale Docente/non Docente solo per uso didattico e/o di formazione. Chiunque acceda ad internet risponde sul piano civile e penale, secondo legislazione vigente, per l'uso del servizio.

Norma generale

I Responsabili dei Laboratori Informatici che rilevino irregolarità nell'uso dei Laboratori stessi sono tenuti a darne tempestiva comunicazione al Dirigente Scolastico.

12 - UTILIZZO DEL TELEFONO CELLULARE E DI DISPOSITIVI ELETTRONICI DURANTE LE ATTIVITÀ SCOLASTICHE

Non è consentito usare i telefoni cellulari durante le attività scolastiche, se non in casi particolari e autorizzati dal Dirigente Scolastico.

Qualora gli alunni abbiano con sé il telefono cellulare, sono tenuti a consegnarlo al personale scolastico all'inizio delle lezioni e a ritirarlo al termine dell'orario scolastico. I cellulari consegnati sono custoditi presso l'Ufficio di Presidenza, in contenitori specifici. Nel caso gli alunni vengano sorpresi mentre usano il cellulare, i Docenti procedono alla requisizione temporanea del dispositivo, lo depositano in Presidenza (nei plessi distaccati lo collocano in posto sicuro e avvertono immediatamente la Sede Centrale) e tramite Segreteria avvisano tempestivamente la Famiglia. I Genitori vengono dunque convocati nella sede scolastica per il ritiro del cellulare temporaneamente trattenuto.

Un uso illegale del cellulare da parte degli alunni (scatto di foto/riprese video non autorizzate/accesso ai social network/atti di cyberbullismo) durante l'orario scolastico comporta la configurazione di reati per i quali non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza, principalmente alla Polizia Postale e delle Comunicazioni.

L'uso da parte degli alunni di dispositivi di memoria esterna (ad esempio di chiavette USB) è consentito, previa autorizzazione del docente, solo nel rispetto delle condizioni seguenti:

- Il dispositivo deve essere acquistato o formattato per un uso esclusivamente scolastico;
- I dispositivi sono consegnati all'insegnante all'inizio e restituiti al termine dell'anno scolastico .

L'uso di dispositivi personali (*computer, tablet, cellulare...*) da parte del Personale Docente è consentito durante l'orario di servizio solo per usi didattici o relativi alla funzione docente. È permesso l'uso del cellulare per comunicazioni personali solo di carattere urgente.

13 - GESTIONE DELL'INFRASTRUTTURA E DELLE DOTAZIONI TECNOLOGICHE DELL'ISTITUTO

Si puntualizzano alcuni aspetti legati alle situazioni seguenti:

- gestione accessi
- uso E-mail
- sito web dell'Istituto
- social network
- protezione dei dati personali
- strumentazione personale

Gestione accessi:

Per quanto riguarda la componente dei Docenti, una buona parte delle sedi dell'Istituto è dotata di una rete WI-FI che consente l'accesso a Internet da qualsiasi postazione scolastica o da dispositivo personale. La rete WI-FI è gestita e monitorata costantemente dall'Animatore Digitale e/o dai Fiduciari di Plesso, anche in base ad eventuali segnalazioni di malfunzionamento da parte dei Docenti.

Uso E-mail:

L'account di posta elettronica della scuola è solo quello istituzionale gestito quotidianamente dagli uffici amministrativi. È in fase di pianificazione il collegamento dell'account di posta elettronica istituzionale con tutte le sedi associate. L'Istituto si compone di 9 scuole d'infanzia, 6 scuole primarie, 3 scuole secondarie di primo grado, dislocate a Voghera e in altri Comuni limitrofi. L'invio/ricevimento di posta elettronica a scopi didattici avviene previa informativa al Dirigente Scolastico e si effettua con il supporto del personale amministrativo.

Sito Web dell'Istituto:

Tutti i contenuti sono pubblicati dall'Animatore Digitale, con invio diretto dei materiali al suo indirizzo mail oppure tramite il personale amministrativo.

Social network:

Attualmente non si usano *social media* e nella prassi didattica quotidiana. L'Istituto non risulta registrato ad alcun social network (Facebook/Instagram/Twitter...). Presso la scuola secondaria di 1° grado Pascoli, è attivo un progetto di sperimentazione di classe virtuale su piattaforma EDMODO.

Protezione dei dati personali:

Il personale scolastico è incaricato del trattamento dei dati personali nei limiti determinati dallo svolgimento della propria funzione. Ai Genitori viene fornita informativa e richiesta di autorizzazione all'utilizzo dei dati personali mediante una specifica modulistica.

14 - PROCEDURE OPERATIVE PER LA PROTEZIONE DEI DATI PERSONALI

È attualmente in uso un modulo di Liberatoria Privacy per trattamento dati personali ed uso immagini e video, suscettibile di futuri adeguamenti (cfr Regolamento UE 679/2016)).

14 - PROCEDURE OPERATIVE PER LA RILEVAZIONE, IL MONITORAGGIO E LA GESTIONE DELLE SEGNALAZIONI

Manifestazioni di cyberbullismo e di lesione della Web Reputation

Flaming: litigi on line con uso di linguaggio violento e volgare

Harassment: molestie tramite invio ripetuto di messaggi 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 all'interno di comunità virtuale di pettegolezzi e commenti denigratori

Outing estorto: registrazione delle confidenze raccolte all'interno di un ambiente privato e poi inserite in "piazze virtuali"

Impersonificazione: sostituzione di persona con l'obiettivo di inviare messaggi ingiuriosi che possano screditare la vittima

Esclusione: estromissione intenzionale dall'attività *on-line*

Sexting: invio di messaggi via cellulare ed internet contenenti immagini a sfondo sessuale.

I Docenti giocano un ruolo importante nel rilevare in forma diretta e/o indiretta eventuali manifestazioni inquadrabili come atti di cyberbullismo, attraverso l'osservazione quotidiana delle relazioni interpersonali tra alunni e delle possibili dinamiche conflittuali all'interno del contesto classe. Gli insegnanti possono inoltre svolgere un'efficace opera di sensibilizzazione su alunni e genitori allo scopo di fare chiarezza su alcuni concetti fondamentali, come la differenza tra "scherzo" e/o litigio e prepotenza/reato. Si sottolinea l'utilità di pianificare e realizzare progetti mirati, integrati, destinati ad alunni e famiglie, che contemplino il supporto di Forze dell'Ordine, Enti ed Associazioni territoriali.

Come segnalare eventuali atti di cyberbullismo

La segnalazione va inoltrata al Dirigente Scolastico, mediante comunicazione orale/scritta riservata. Il Dirigente Scolastico potrà in seguito avvalersi del supporto del Referente d'Istituto per la prevenzione e il contrasto al cyberbullismo, dei propri Collaboratori, dell'Animatore Digitale. Per gli *step* successivi, il Dirigente Scolastico potrà orientare il proprio intervento in due direzioni:

1. Prendere contatti con il CORECOM (Comitato Regionale per le Comunicazioni della Regione Lombardia), limitatamente ai casi che non risultino di competenza dell'Autorità Giudiziaria.

Sito: www.corecomlombardia.it

E-mail: sportellowebreputation@consiglio.regione.lombardia.it

Tel. 02 67482725

2. Contattare le Forze dell'Ordine, prioritariamente la Polizia Postale e delle Comunicazioni.

Sito: <https://www.commissariatodips.it/>

Abusi sessuali

L'abuso sessuale risulta amplificato, nella società odierna, dall'opportunità d'uso del *web*. È possibile scaricare o vendere immagini/filmati di pornografia infantile, all'interno di siti *web* "oscuri". Un adulto può contattare minorenni sotto la copertura

di una falsa identità, tramite *chat* e *social*. In alcuni casi di disagio socio-economico gli stessi genitori possono indurre i propri figli a spogliarsi davanti alla *webcam*. I Docenti svolgono un ruolo molto delicato di osservatori degli eventuali "campanelli d'allarme" (alterazioni del comportamento, riferimenti a vissuti di natura sessuale in resoconti orali/scritti, segni fisici di violenza...), in sinergia con gli altri operatori scolastici, con il Dirigente Scolastico, con i consulenti esterni di Enti Locali (assistenti sociali/operatori sanitari) e di associazioni territoriali.

Come segnalare eventuali abusi sessuali

In caso di reperimento su Internet di materiale pedopornografico, è necessario evitare il *download*, la produzione di copie, la condivisione di *link* o il postarne il contenuto. Occorre invece segnalare la presenza dei materiali individuati alla Polizia Postale e delle Comunicazioni (Sito: <https://www.commissariatodips.it/>) oppure a siti specializzati nella loro eliminazione (www.stop-it.it, www.azzurro.it...). È infine possibile recarsi personalmente nella più vicina sede di Polizia Giudiziaria.

15 - PROCEDURE OPERATIVE PER LA GESTIONE DEI CASI

Linee guida per gli Alunni

- Non comunicare a nessuno le tue *password* e cambiale periodicamente, usando numeri, lettere e caratteri speciali;
- non divulgare nome/cognome, indirizzo, telefono di casa, nome e indirizzo della tua scuola;
- non inviare a sconosciuti fotografie tue o di tuoi amici;
- prima di inviare via *web* la fotografia di qualcuno, chiedi il permesso di farlo;
- chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da internet;
- quando sei nel *web* rispetta sempre gli altri, esiste anche la "WEB REPUTATION";
- non rispondere alle offese e agli insulti;
- segnala, con l'assistenza dei tuoi Genitori e dei tuoi Insegnanti, la presenza di cyberbulli;
- conserva le comunicazioni offensive, sono prove per future segnalazioni/denunce;
- se ricevi materiale offensivo, non diffonderlo: potresti essere accusato di complicità;
- rifletti prima di inviare qualsiasi cosa: ricorda che tutto ciò che invii su internet diviene pubblico e rimane per sempre;
- se qualcuno su internet ti chiede un incontro di persona, riferiscilo al tuo insegnante e ai tuoi genitori;
- ricorda che le persone incontrate su internet non sempre sono quello che dichiarano di essere;
- non scaricare o copiare materiale da internet senza il permesso del tuo insegnante e/o dei tuoi genitori;
- non caricare materiali nei siti *web* senza il permesso del tuo insegnante e/o dei tuoi genitori.

Linee guida per gli Insegnanti

- Evitate di lasciare *file* personali sui *computer* della scuola;
- salvate i vostri lavori in cartelle personali e/o di classe e non sul *desktop*;
- illustrate agli alunni i concetti fondamentali della *E-Policy* d'Istituto. Discutete con loro di utilizzo consentito della Rete, di comportamenti corretti/illeciti nelle chat e nei social media;
- fornite indicazioni d'uso di internet, avvertite che le navigazioni saranno controllate;
- ricordate di chiudere la connessione al termine della sessione di lavoro su internet;
- ricordate agli alunni che la violazione della *E-Policy* comporta sanzioni di vario genere;
- adottate provvedimenti disciplinari condivisi con i colleghi e approvati nelle sedi istituzionali (Collegio Docenti/Consiglio d'Istituto);
- attivate progettualità volte a rinforzare i comportamenti corretti e riparativi, la gestione positiva dei conflitti, la promozione dei rapporti amicali e della solidarietà, la personale maturazione emotivo-affettiva;
- nelle situazioni problematiche condividete le strategie adottabili con il Consiglio di Classe, con il Dirigente Scolastico e convocate i Genitori, per valutare a quali risorse territoriali possano rivolgersi;
- in caso di atti di cyberbullismo, seguite la procedura indicata nel presente documento di *E-Policy*;
- segnalate la presenza di materiale pedopornografico alla Polizia Postale e delle Comunicazioni o ai siti specializzati (Telefono Azzurro...);
- in caso di abuso sessuale rilevato anche attraverso le nuove tecnologie, informate in via prioritaria il Dirigente Scolastico per l'attivazione delle necessarie procedure di legge (denuncia alle Forze dell'Ordine).

Linee guida per i Genitori sull'uso di internet

- Informati costantemente sulle novità tecnologiche: al giorno d'oggi molti bambini rischiano di maneggiare in età precoce dispositivi di cui non comprendono il potere;
- non mentire sull'età di tuo figlio per iscriverlo ad un *social network*, scaricare un'app, o iscriversi ad un videogioco: i limiti d'età sono una garanzia di protezione;
- non cedere sulle regole che decidi di adottare;
- metti il pc ad uso di tuo figlio in un posto visibile e controllabile;
- molti dispositivi moderni hanno dei controlli parentali già inclusi, ad esempio sugli orari di accesso o sulla selezione dei siti internet da bloccare;
- monitora i *social network*: un *post* rimane in rete per sempre. Attualmente i datori di lavoro controllano anche i profili sui *social*, per cui è bene educare precocemente i figli ad un uso consapevole di internet, su cosa è sbagliato pubblicare *on line* e sul profilo personale;
- parla con i tuoi figli e naviga su internet con loro. Educali su confini, reputazione, rischi;
- aiuta i tuoi figli a proteggere i loro *device* e *account*. Insegna loro come creare una *password* efficiente, a non condividerla con nessuno, ma solo con te, a valutarne l'importanza (*password* lunghe almeno 8 caratteri, senza date importanti o riferimenti alla propria realtà. Blocco di ogni *device* con una *password*. Uso di *password* diverse per un *social*, per la posta, uso di una *passphrase*);

- ricorda ai più piccoli di non condividere informazioni personali *on line*, come età, scuola, indirizzo, numero di telefono, o qualsiasi dato che li renda identificabili. Considera anche il rischio che possano essere individuati secondo la loro posizione: disattiva il *geotagging* sulle loro fotografie, assicurati che non condividano la loro posizione GPS con sconosciuti;
- parla del *sexting*: verifica che i tuoi figli, specie se adolescenti, conoscano i rischi a cui vanno incontro, e le conseguenze legali. Ricorda che le foto a sfondo sessuale, una volta inviate in Rete, vanno fuori controllo, non si possono più eliminare, con ripercussioni sul loro futuro;
- ogni *software* (specie sistemi operativi, *browser internet*, antivirus) deve essere aggiornato regolarmente per evitare che qualcuno possa infiltrarsi e rubare dati personali. Usa anche sistemi di *backup* esterni per salvare fotografie e documenti importanti.

16 - FORMAZIONE E CURRICOLO

Il curriculum di studi degli studenti

Coerentemente con il PTOF dell'Istituto, la scuola pone come traguardo fondante l'acquisizione da parte degli alunni della capacità di utilizzare in modo autonomo i dispositivi tecnologici per attività di studio e ricerca e lo sviluppo di consapevolezza e senso critico nella navigazione in internet.

"[...] connotativa della Vision d'Istituto è la scelta di avvicinare precocemente gli alunni all'uso consapevole delle nuove tecnologie, per acquisire quelle competenze digitali che rappresentano un fondamentale passaporto per ogni possibile percorso formativo futuro." [PTOF 2017-2019].

Alla costruzione di queste competenze concorrono l'azione didattica mirata durante le ore curricolari di Tecnologia e l'inserimento trasversale, nelle diverse discipline, di azioni educative volte a far conoscere e padroneggiare agli alunni il potenziale delle tecnologie digitali e di internet nei processi di costruzione della conoscenza e alla costruzione di consapevolezza e senso critico rispetto ai rischi ad esse connessi.

La formazione del personale docente

Sulla base delle segnalazioni pervenute dall'Animatore Digitale, dal Referente d'Istituto per la prevenzione ed il contrasto del cyberbullismo e dai Fiduciari di Plesso, la scuola provvede a garantire ai docenti l'attivazione o l'accesso a corsi di formazione e aggiornamento necessari per un utilizzo corretto e consapevole di internet e delle TIC e per la salvaguardia degli alunni rispetto ai rischi connessi al loro uso.

L'informazione dei genitori

La scuola organizza nel corso dell'anno scolastico incontri con esperti rivolti ai genitori e ai docenti per favorire la riflessione comunitaria sui temi di rilevanza e attualità (es. cyberbullismo, dipendenza dai media, gioco d'azzardo...) al fine di costruire e consolidare la comunità educante.

