ISTITUTO COMPRENSIVO COSTIGLIOLE

Piazza Medici n. 1 - 14055 COSTIGLIOLE D'ASTI

Tel. 0141 966054 Fax 0141 962691

atic81200t@istruzione.it atic81200t@pec.istruzione.it

www.iccostigliole.gov.it

E-Safety Policy

Anno Scolastico 2015-2016

Sommario

E-Safety Policy 1
1. Introduzione 3
1.1 Scopo della Policy. 3
1.2 Ruoli e Responsabilità della Comunità Scolastica. 3
1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica. 5
1.4 Gestione delle infrazioni alla Policy. 6
1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento. 7
1.6 Integrazione della Policy con Regolamenti esistenti. 7
2. Formazione e Curricolo 7
2.1. Curricolo sulle competenze digitali per gli studenti. 7
2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica. 10
2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali. 11
2.4 Sensibilizzazione delle famiglie. 11
3. Gestione dell'infrastruttura e della strumentazione ICT della scuola. 11
3.1 Accesso ad internet: filtri, antivirus e sulla navigazione. 11
3.2 Gestione accessi (password, backup, ecc.). 12
3.3. E-mail. 12
3.4 Blog e sito web della scuola 12
3.5 Social network. 13
3.6 Protezione dei dati personali. 13
4. Strumentazione personale 13
4.1 Gestione degli strumenti personali 13
5. Prevenzione, rilevazione e gestione dei casi 15
Prevenzione: 15
Azioni: 15

1. Introduzione

"la diffusione delle tecnologie di informazione e di comunicazione è una grande opportunità e rappresenta la frontiera decisiva per la scuola. Si tratta di una rivoluzione epocale, non riconducibile a un semplice aumento dei mezzi implicati nell'apprendimento".

(Indicazioni Nazionali per il curricolo, 2012)

Le TIC e nuovi media sono entrati prepotentemente a far parte della vita della maggior parte dei pre-adolescenti e adolescenti italiani, supportando e facilitando la comunicazione e, potenzialmente, la collaborazione. Rappresentano uno strumento essenziale di emporwerment, di espressione e partecipazione che influenza la società e la vita personale degli individui di ogni età, ma in particolare dei più giovani. La partecipazione basata sulle tecnologie dell'informazione e della comunicazione deve essere collocata nel quadro dei diritti dei bambini e dei ragazzi, che comprendono la parità di accesso, la trasparenza, il diritto alla privacy, alla libertà di espressione, i quali però devono contemporaneamente essere tutelati nel loro diritto ad essere ad essere protetti da abusi e violenze (artt. 19-34 della CRC).

1.1 Scopo della Policy.

La presenza sempre più diffusa di tecnologie digitali anche all'interno degli ambienti scolastici pone in essere nuove necessità e attenzioni relative al loro uso sicuro, consapevole e positivo, in particolare per quanto riguarda l'uso di nuove TIC nella didattica e l'implementazione e la diffusione della rete internet (anche Wi-Fi).

La comunità scolastica nel suo complesso è chiamata a svolgere un ruolo fondamentale nel garantire che bambini/e e adolescenti siano in grado di utilizzare le tecnologie digitali in modo appropriato e sicuro.

E' in questo quadro che s'inserisce la necessità di affrontare la questione da più punti di vista coinvolgendo più interlocutori al fine di dotare la nostra comunità scolastica di una propria Policy di E-safety che definisca:

1. misure di prevenzione e di gestione di situazioni problematiche relative all'uso delle tecnologie digitali;
2. Misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici.

L'E-safety della scuola fa quindi riferimento a un insieme di regolamenti, linee di azione e attività che verranno poste in essere per fare fronte ad una serie di necessità individuate e che andranno a corroborare gli altri regolamenti d'istituto e le politiche relative ai comportamenti degli alunni.

Una policy non è mai il risultato di un'azione unica, quanto piuttosto l'esito delle interazioni di un insieme di azioni e decisioni.

(Generazioni connesse)

1.2 Ruoli e Responsabilità della Comunità Scolastica

Al fine di garantire interventi mirati e tempestivi di tutela, in caso di episodi di "abusi on line", e/o di sanzione in caso di mancata osservazione dei regolamenti vengono qui definiti in modo chiaro ed univoco ruoli e responsabilità dei membri della comunità scolastica.

L'istituto ha costituito un gruppo di lavoro che si occupa della stesura e del monitoraggio dell'E-safety policy, approvata dal Collegio dei docenti e dal Dirigente scolastico.

L’E-safety Policy verrà revisionata ogni anno.

RUOLO	RESPONSABILITÀ
Dirigente scolastico	• Responsabilità globale della e-safety • Responsabilità dei dati sensibili e dati relativi alla sicurezza • Assicurare che la scuola utilizzi un Internet Service approvato, filtrato, che è conforme ai requisiti di legge • Assicurare che il personale addetto alla sicurezza su internet riceva una formazione adeguata per svolgere il proprio compito • Essere a conoscenza delle procedure da seguire in caso di eventuali incidenti (e-safety). • Ricevere relazioni periodiche di monitoraggio dal Coordinatore / Responsabile (e-sicurezza) • Garantire che vi sia un sistema in grado di monitorare e supportare il personale che svolge le procedure di e-sicurezza interna (ad esempio, gestore della rete.)

Coordinatore gruppo E-safety/Animatore Digitale	• Coordinare e mantenere contatti con il gruppo di lavoro, autorità e gli enti esperti.
	• Relazionare periodicamente il lavoro del gruppo con la dirigenza.
	• Revisionare periodicamente e aggiorna il registro degli incidenti
	• Tenersi aggiornato riguardo alla legislazione in materia di e-safety ed è consapevole dei potenziali gravi problemi derivati da:
	  o Condivisione di dati personali
	  o L'accesso ai materiali illegali / inadeguati
	  o Inadeguato contatto on-line con adulti / sconosciuti
	  o Incidenti potenziali o reali di adescamento
	  o Cyber-bullismo e uso dei social media

Gruppo di lavoro E-safety	• Definire e revisionare le politiche e i documenti di e-safety
	• Promuovere la consapevolezza e l'impegno per la salvaguardia relativa alle tecnologie di tutta la comunità scolastica.
	• Operare affinché tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso d’incidenti
	• Assicurare che nel curricolo scolastico vengano inseriti i vari aspetti della sicurezza in internet.
	• Tenersi aggiornato riguardo alla legislazione in materia di e-safety ed è consapevole dei potenziali gravi problemi derivati da:
	  o Condivisione di dati personali
	  o L'accesso ai materiali illegali / inadeguati
	  o Inadeguato contatto on-line con adulti / sconosciuti
	  o Incidenti potenziali o reali di adescamento
	  o Cyber-bullismo e uso dei social media

Staff	• Contribuire a promuovere politiche di e-safety della scuola • Essere consapevole dei problemi di sicurezza correlati all'uso di telefoni cellulari, fotocamere e dispositivi portatili, ne monitora l'utilizzo e applica le vigenti politiche scolastiche in materia.

	• Segnalare qualsiasi abuso sospetto o problema al coordinatore di e-safety • Favorire comportamenti sicuri, responsabili e professionali nell'utilizzo della tecnologia. • Garantire che le comunicazioni digitali con gli allievi avvengano in modo professionale e solo attraverso sistemi adottati e approvati dalla scuola
Insegnanti	• Informare gli alunni sui rischi della rete e sulla politica di E-safety adottata dall'istituto. • Informare gli alunni sugli aspetti giuridici riguardanti i contenuti elettronici, quali le leggi sul copyright, la privacy, ecc. • Supervisionare e guidano gli alunni nelle attività di apprendimento che coinvolgono tecnologia on-line. • Incorporare i temi di e-safety e di competenza digitale, in modo trasversale a tutte le attività scolastiche.
Tecnico	• Fare una manutenzione periodica delle apparecchiature e del sistema di filtraggio dei dati.
Studenti	• Leggere, comprendere e aderire all'E-safety Policy della scuola e al patto di corresponsabilità • Utilizzare le TIC ai fini delle attività scolastiche evitando il plagio e rispettando le normative sul diritto d'autore • Comprendere l'importanza di segnalare abusi, usi impropri o l'accesso a materiali inappropriati. • Venire informati su quali azioni intraprendere nel caso in cui loro stessi o qualcuno di loro conoscenza si trovi in situazione di rischio o disagio. • Conoscere e comprendono la politica della scuola sull'uso dei telefoni cellulari, fotocamere digitali e dispositivi portatili. • Conoscere e capiscono la politica scolastica relativa all'uso d'immagini e di cyber-bullismo. • Conoscere i vantaggi e i rischi dell'utilizzo di Internet e delle altre tecnologie.
Genitori	• Leggere, comprendere, firmare e aderire all'E-safety Policy della scuola e al patto di corresponsabilità. • Sostenere la scuola nel promuovere e-safety. • Leggere, comprendere e promuovere l'accordo che l'allievo sottoscrive con la scuola riguardo all'e-safety. • Consultarsi con la scuola se hanno qualche preoccupazione riguardo all'uso della tecnologia da parte dei loro figli. • Partecipare alle iniziative di formazione in materia di sicurezza in rete promosse dall'istituto.

1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica.

Per far si che si diffonda fra tutti i membri della comunità scolastica un corretto uso delle TIC e della rete e per diffondere consapevolezza su norme e sanzioni, l'E-Safety Policy verrà condivisa con l'intera comunità scolastica avvalendosi di diversi mezzi:

PERSONALE DOCENTE E ATA

- Comunicazioni interne/circolari
- Informazione e discussione al Collegio Docenti
- Pubblicazione sul Sito Web d'Istituto - Regolamenti
- Distribuzione di una copia di E-Safety Policy in ogni plesso per la libera consultazione

ALUNNI

- Affissione in ogni aula delle regole per l'accesso a Internet anche con dispositivi personali
- Discussione della E-Safety Policy in classe (scuola primaria e secondaria I°)
- Inserimento estratto E-Safety Policy d'istituto nel diario scolastico

GENITORI

- Pubblicazione della versione integrale della E-Safety Policy sul sito web d'istituto
- Inserimento dell'E-Safety Policy nel diario di ogni alunno
- Condivisione con le famiglie dell'adozione di questo nuovo regolamento nelle riunioni d'inizio anno

1.4 Gestione delle infrazioni alla Policy.

Mancanza Disciplinare	Frequenza	Provvedimento	Organo
Lo studente usa il cellulare senza il consenso del docente.	a) 1° volta	Nota sul diario, ritiro del cellulare, consegna all'alunno alla fine delle lezioni e colloquio con i genitori	Docente Dirigente Scolastico o suo collaboratore.
	b) dalla 2° Volta in poi	Nota sul registro di classe, ritiro del cellulare e consegna alla fine delle lezioni. Colloquio con l'alunno e i genitori. Provvedimento del Dirigente di richiamo scritto con assegnazione di eventuali attività socialmente utili da svolgere a scuola. Per infrazioni reiterate, sospensione dalle lezioni per uno o più giorni. Ricadute sul voto di comportamento.	Docente Dirigente Scolastico Consiglio di classe Consiglio di Istituto
Lo studente utilizza il cellulare o altro dispositivo. Lo studente acquisisce in ambito scolastico, con il cellulare o con altro dispositivo, dati personali (immagini, suoni, filmati) e li diffonde nella rete o a terzi, senza autorizzazione dei diretti interessati.		Nota sul registro di classe, ritiro del cellulare e consegna alla fine delle lezioni. Colloquio con l'alunno e i genitori. Provvedimento del Dirigente di richiamo scritto con assegnazione di eventuali attività socialmente utili da svolgere a scuola. Per infrazioni reiterate, sospensione dalle lezioni per uno o più giorni. Ricadute sul voto di comportamento.	Docente Dirigente Scolastico Consiglio di classe Consiglio di Istituto

1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento.

La Policy verrà monitorata tramite l'utilizzo di un apposito registro e verrà revisionata e aggiornata ogni anno dal gruppo di lavoro alla luce delle esigenze emerse.

1.6 Integrazione della Policy con Regolamenti esistenti.

La policy verrà integrata con il regolamento d'istituto e il patto educativo in vigore.

2. Formazione e Curricolo

2.1. Curricolo sulle competenze digitali per gli studenti.

La competenza digitale fa riferimento alla capacità di comprendere e sfruttare l'effettivo potenziale delle tecnologie in ottica di costruzione di conoscenza e di promozione della partecipazione e dell'inclusione; il rapporto con le tecnologie digitali guarda così a forme di uso consapevole, critico e creativo.

L'Istituto Comprensivo Costigliole ha elaborato un proprio curricolo per lo sviluppo delle competenze digitali, così come previsto dalle Indicazioni Nazionali che identificano il quadro delle competenze-chiave per l'apprendimento permanente definite dal Parlamento europeo e dal Consiglio dell'Unione europea come l'orizzonte di riferimento verso cui il sistema scolastico italiano tende.

Tra le competenze-chiave è elencata anche la competenza digitale che, così come precisato dalle Indicazioni Nazionali, rappresenta un elemento fondamentale di ogni disciplina.

Nella scuola primaria attraverso la disciplina "tecnologia" si può promuovere l'integrazione delle conoscenze teoriche con quelle pratiche che concorrono alla comprensione di sistemi complessi; si sottolinea, inoltre, che, per quanto riguarda le tecnologie dell'informazione e della comunicazione e le tecnologie digitali, oltre alla padronanza degli strumenti, è necessario sviluppare un atteggiamento critico ed una consapevolezza rispetto agli effetti sociali e culturali della loro diffusione, alle conseguenze relazionali e psicologiche dei possibili modi d'impiego, alle ricadute di tipo ambientale o sanitario. Si riconosce che quest'ultimo compito educativo, in particolare, deve essere condiviso tra tutte le discipline.

Nella scuola secondaria di primo grado la competenza digitale è annoverata ancora tra le competenze trasversali necessarie alla cittadinanza; non è previsto un curriculum specifico ed unitario dedicato ai linguaggi mediali e alla competenza digitale, ma solamente il riferimento a obiettivi di apprendimento e traguardi di competenze nelle diverse aree disciplinari.

Allo stato attuale quindi la competenza digitale va a configurarsi non come disciplina autonoma, ma come ambito che gli alunni possono sviluppare in maniera trasversale nel complesso delle attività didattiche.

COMPETENZA CHIAVE EUROPEA: COMPETENZA DIGITALE - DISCIPLINE DI RIFERIMENTO: tutte

	FINE CLASSE TERZA SCUOLA PRIMARIA	
COMPETENZE SPECIFICHE	**ABILITA'**	**CONOSCENZE**
Utilizzare le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo.	Utilizzare il PC, con la supervisione dell'insegnante, per scrivere, compilare tabelle e disegnare. Utilizzare alcune funzioni principali, come creare un file, caricare immagini, salvare il file.	Uso di Word e di Paint. Funzionamento elementare del PC.
Avviare ad una prima consapevolezza delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione.	Individuare alcuni rischi fisici nell'uso di apparecchiature elettriche ed elettroniche e ipotizzare soluzioni preventive. Individuare alcuni rischi nell'utilizzo della rete Internet e ipotizzare alcune semplici soluzioni preventive.	Rischi fisici nell'utilizzo di apparecchi elettrici ed elettronici. Rischi nell'utilizzo della rete con PC.
	FINE SCUOLA PRIMARIA	
	ABILITA'	**CONOSCENZE**
Utilizzare le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili a un dato contesto applicativo.	Utilizzare il PC, alcune periferiche e programmi applicativi. Utilizzare semplici materiali digitali per l'apprendimento. Avviare alla conoscenza della Rete per scopi d'informazione, comunicazione, ricerca e svago.	I principali dispositivi informatici d'input e output. I principali software applicativi utili per lo studio, con particolare riferimento alla videoscrittura, al disegno e ai giochi didattici. Semplici procedure di utilizzo di Internet per ottenere dati, fare ricerche, comunicare.
Avviare a una prima consapevolezza delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione.	Individuare rischi fisici nell'utilizzo delle apparecchiature elettriche ed elettroniche e i possibili comportamenti preventivi. Individuare i rischi nell'utilizzo della rete Internet e individuare alcuni comportamenti preventivi e correttivi.	Rischi fisici nell'utilizzo di apparecchi elettrici ed elettronici Rischi nell'utilizzo della rete con PC e cellulari
	FINE SCUOLA SECONDARIA DI PRIMO GRADO	

COMPETENZE SPECIFICHE	ABILITA'	CONOSCENZE
Utilizzare con dimestichezza le più comuni tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili a un dato contesto applicativo, a partire dall'attività di studio.	Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti in diverse situazioni. Conoscere gli elementi basilari che compongono un computer e le relazioni essenziali fra di essi. Collegare (Mettere in relazione) le modalità di funzionamento dei dispositivi elettronici con le conoscenze scientifiche e tecniche acquisite. Utilizzare materiali digitali per l'apprendimento. Utilizzare il PC, periferiche e programmi applicativi Utilizzare la rete per scopi d'informazione, comunicazione, ricerca e svago.	I dispositivi informatici d'input e output Il sistema operativo e i più comuni software applicativi, con particolare riferimento all'office automazioni e ai prodotti multimediali anche Open source. Procedure per la produzione di testi, ipertesti, presentazioni e utilizzo dei fogli di calcolo. Procedure di utilizzo di reti informatiche per ottenere dati, fare ricerche, comunicare. Caratteristiche e potenzialità tecnologiche degli strumenti d'uso più comuni.
Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto in cui vengono applicate.	Riconoscere potenzialità e rischi connessi all'uso delle tecnologie più comuni, anche informatiche.	Procedure di utilizzo sicuro e legale di reti informatiche per ottenere dati e comunicare (motori di ricerca, sistemi di comunicazione mobile, email, chat, social network, protezione degli account, download, diritto d'autore, ecc.). Fonti di pericolo e procedure di sicurezza.
LIVELLI DI PADRONANZA		
LIVELLO 1	Sotto la diretta supervisione dell'insegnante identifica, denomina e conosce le funzioni fondamentali di base dello strumento. Con la supervisione dell'insegnante, utilizza i principali componenti, in particolare la tastiera. Comprende e produce semplici frasi associandole ad immagini date..	
	Sotto la diretta supervisione dell'insegnante e con sue istruzioni, scrive un	

LIVELLO 2	semplice testo al computer e lo salva. Utilizza la rete solo con la diretta supervisione dell'adulto per cercare informazioni.
LIVELLO 3 ***atteso a partire dalla fine della scuola primaria***	Scrive, revisiona e archivia in modo autonomo testi scritti con il PC. Costruisce tabelle di dati con la supervisione dell'insegnante. Comprende semplici testi inviati da altri via mail; con l'aiuto dell'insegnante, trasmette semplici messaggi di posta elettronica. Accede alla rete con la supervisione dell'insegnante per ricavare informazioni. Conosce e descrive alcuni rischi della navigazione in rete e dell'uso del cellulare e adotta i comportamenti preventivi.
LIVELLO 4 ***atteso nella scuola secondaria di primo grado***	Scrive, revisiona e archivia in modo autonomo testi scritti con il PC; è in grado di modificarli, inserendo immagini, disegni, tabelle. Costruisce tabelle di dati; utilizza fogli elettronici per semplici elaborazioni di dati e calcoli. Utilizza la posta elettronica e accede alla rete con la supervisione dell'insegnante per ricavare informazioni e per collocarne di proprie. Conosce e descrive i rischi della navigazione in rete e dell'uso del cellulare e adotta i comportamenti preventivi.
LIVELLO 5 ***Atteso alla fine della scuola secondaria di primo grado***	Utilizza in autonomia programmi di videoscrittura, fogli di calcolo, presentazioni per elaborare testi, comunicare, eseguire compiti e risolvere problemi. Sa utilizzare la rete per reperire informazioni, con la supervisione dell'insegnante; organizza le informazioni in file, schemi, tabelle, grafici; collega file differenti. Confronta le informazioni reperite in rete anche con altre fonti documentali, testimoniali, bibliografiche. Comunica autonomamente attraverso la posta elettronica. Rispetta le regole della netiquette nella navigazione in rete e sa riconoscere i principali pericoli della rete (spam, falsi messaggi di posta, richieste di dati personali, ecc.), contenuti pericolosi o fraudolenti, evitandoli.

2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.

Il concreto utilizzo delle Tic in classe come elemento innovativo non dipende solamente dall'effettiva e funzionale dotazione strumentale, ma anche e soprattutto dalla capacità di comprenderne le potenzialità rispetto a contesti e finalità specifici. Per sostenere un processo di consapevole innovazione didattica è

necessario investire sulla formazione e l'aggiornamento degli insegnanti. La nostra scuola supporta la formazione dei docenti in servizio attraverso:

- L'organizzazione di corsi interni con relativo catalogo
- La partecipazione a reti di scuole che effettuano anche percorsi di formazione
- La diffusione tramite sito web d'informazioni su corsi sia gratuiti sia a pagamento organizzati da diversi enti
- Nel corso degli anni i docenti hanno partecipato a corsi su:
- Percorsi ForTic I e II
- Utilizzo delle LIM in classe
- Conseguimento ECDL
- Uso delle tecnologie per la didattica
- Uso delle tecnologie per una didattica inclusiva
- Pensiero computazionale – coding

2.3 Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

L'implementazione della rete internet nella scuola - in particolare il wifi - rende ancor più pressante la necessità di formare i docenti sull'uso consapevole di internet e sui rischi della rete. La nostra scuola supporta la formazione e l'aggiornamento dei docenti in tal senso attraverso:

- l'organizzazione di corsi interni con relativo catalogo
- la partecipazione a reti di scuole che effettuano anche percorsi di formazione (bando cyberbullismo)
- la diffusione tramite sito web di informazioni su corsi sia gratuiti sia a pagamento organizzati da diversi enti [corsi castigliano su cyberbullismo….]

2.4 Sensibilizzazione delle famiglie.

Gli adulti devono assicurare l'opportunità a bambini e ragazzi di utilizzare in modo sicuro e consapevole i nuovi media, ed è proprio a tal fine che l'istituto organizza da anni incontri di sensibilizzazione aperti alle famiglie, anche con la collaborazione di associazioni del territorio e della polizia postale. Gli incontri si strutturano in dimostrazioni/lezioni con esperti del settore in cui vengono forniti suggerimenti per l'uso di Internet e delle tecnologie. Negli anni si sono consolidate esperienze di vario tipo:

- Partecipazione a seminari di Move up - destinazioni alternative - Educare tra reale e virtuale
- Collaborazione con la Polizia Postale
- Collaborazione con l'associazione Mani Colorate - progetto informi@moci
- Centro di documentazione Steadycam - serate informative per genitori e docenti su Internet, Social Network, nuove tecnologie e mondo dei videogiochi

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola.

3.1 Accesso ad internet: filtri, antivirus e sulla navigazione.

- L'uso di Internet è consentito esclusivamente per la comunicazione scolastica e la ricerca d'informazioni per fini scolastici.

- Gli utenti si impegnano a non consultare deliberatamente, conservare o diffondere documenti che possono ledere la dignità della persona, che hanno carattere pornografico, che incitano all'odio razziale o che costituiscono un'apologia del crimine o della violenza (ai sensi degli artt. 173, 197, 261 CPS).
- Non è definito a priori un elenco di siti autorizzati ma è tuttavia permesso l'utilizzo di adeguati strumenti di filtraggio, mediante i quali può essere bloccata la navigazione su categorie di siti i cui contenuti sono stati classificati come potenzialmente pericolosi per l'utenza o certamente estranei agli interessi ed alle attività didattiche.
- I computer della scuola saranno forniti di un sistema di filtraggio che prevede (la scelta e la combinazione di sistemi di filtraggio dipende dalla scuola):
    1. l'accesso bloccato a siti inadeguati;
    2. l'accesso consentito soltanto ad un elenco approvato di siti;
    3. il contenuto delle pagine web/ricerche web filtrato (tramite il riconoscimento di parole sconvenienti);
    4. il monitoraggio della mappa dei siti Internet visitati da studenti e insegnanti. (l'accesso a siti proibiti risulterà da un rapporto che i filtri stessi effettueranno sui siti visitati).
- Viene altresì proibita la possibilità di caricare/scaricare (upload/download) a/da Internet files musicali, video o software che non siano attinenti alla propria mansione, come anche l'utilizzo della connessione ad Internet per motivi strettamente personali.
- Viene tassativamente vietato l'utilizzo delle risorse del server centrale per la memorizzazione di materiale privato e personale.

3.2 Gestione accessi (password, backup, ecc.).

- Il personale scolastico e gli alunni devono mantenere le loro password private, non devono condividerle con gli altri e non devono lasciarle in luoghi dove si possano trovare.
- La connessione ad internet della scuola ha un proprio nome utente e password univoci di accesso. Il personale ha la responsabilità di mantenere questi dati privati.

3.3. E-mail.

- La mail d'istituto è utilizzata solamente per comunicazione di carattere lavorativo.
- Gli utenti si impegnano a non diffondere informazioni che possono nuocere alla reputazione della scuola o essere contrarie alla morale o alle leggi in vigore. Ogni messaggio trasmesso deve recare il nome del suo autore. Non è consentita la pubblicità, in nessuna forma. I dati personali di un adulto non devono essere trasmessi senza il suo accordo; per i dati di minorenni è necessario l'accordo dei genitori.

3.4 Blog e sito web della scuola

Il Dirigente, o persona da questi delegata, si assume la responsabilità di assicurare che:

- il contenuto del sito sia preciso e la qualità della presentazione sia mantenuta;
- il caricamento delle informazioni sul sito sia compito esclusivo dell'autorità delegata a tale compito
- il sito web della scuola sia conforme alle linee guida di legge;
- la maggior parte del materiale è frutto del lavoro della scuola; qualora fosse pubblicato il lavoro di altri verranno rese note le fonti utilizzate e indicata chiaramente l'identità dell'autore;
- i contatti indicati sul sito web siano: l'indirizzo della scuola, il numero di telefono, l'email;
- le foto pubblicate sul web non abbiano un nome completo in allegato;
- non siano usati i nomi degli alunni quando si salvano le immagini nei nomi dei file o dei tag durante la pubblicazione sul sito web della scuola;

Gli utenti si impegnano a non diffondere informazioni che appartengono a terzi senza l'autorizzazione degli stessi (cfr. Legge sul diritto d'autore, LDA, del 9 ottobre 1992) e nei singoli casi si impegnano a menzionare le fonti quando si servono di informazioni di terze persone.

Sono proibite la duplicazione e la diffusione di programmi e documenti coperti dal diritto d'autore.

3.5 Social network.

L'istituto comprensivo per il momento non si avvale dell'uso di social network.

3.6 Protezione dei dati personali.

I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti e non saranno comunicati ad altri soggetti, né saranno oggetto di diffusione. Il responsabile del loro trattamento è il Dirigente scolastico dell'istituto, o persona da questi delegata. In ogni momento è possibile esercitare i propri diritti nei confronti del titolare del trattamento, ai sensi dell'art.7 del D.Lgs.196/2003.

I soggetti cui si riferiscono i dati personali hanno il diritto in qualunque momento di ottenere la conferma dell'esistenza o meno dei medesimi dati e di conoscerne il contenuto e l'origine, verificarne l'esattezza o chiederne l'integrazione o l'aggiornamento, oppure la rettificazione (art. 7 del D.lgs. n. 196/2003). Ai sensi del medesimo articolo gli interessati hanno il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento.

Le richieste vanno rivolte all'Istituto Comprensivo Costigliole, Piazza Medici 1, Costigliole d'Asti (Asti).

4. Strumentazione personale

Uno degli obiettivi tecnologici della scuola è garantire che l'interazione di ogni utente con la tecnologia contribuisca positivamente all'ambiente educativo a scuola. L'uso negativo dei dispositivi tecnologici dentro e fuori la nostra scuola è inaccettabile.

4.1 Gestione degli strumenti personali

- ***Per gli studenti***

1. Agli studenti non è permesso usare i propri dispositivi al di fuori dall'orario di lezione.
2. I dispositivi devono essere usati a scuola per soli scopi didattici SOLTANTO con il consenso esplicito dell'insegnante; agli studenti non è permesso usarli per giochi o attività personali durante le ore scolastiche.
3. Sono ammessi in classe: computer portatili, tablet, smartphone ed e-reader.
4. Ogni studente è responsabile del proprio dispositivo, la scuola non deve essere considerata responsabile della sicurezza dei dispositivi. La scuola non sarà ritenuta responsabile per nessun dispositivo degli studenti lasciato a scuola.
5. Gli studenti non possono prendere in prestito dispositivi di altri studenti.
6. Solamente un dispositivo per studente sarà registrato nel sistema scolastico. Se lo studente ha necessità di cambiare il dispositivo che sta usando e sostituirlo con un altro, il precedente dispositivo verrà cancellato dal sistema scolastico e sostituito con il nuovo.
7. E' vietato agli studenti usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare media o fare foto in classe senza il permesso dell'insegnante e senza il consenso della persona che viene registrata.
8. Audio e video registrati a scuola a fini didattici possono essere pubblicati esclusivamente in canali di comunicazione intestati ufficialmente all'IC di Costigliole d'Asti
9. Agli studenti non è consentito:
    a. usare Internet per scopi diversi da quelli didattici;

   b. scaricare musica, video e programmi da internet senza l'esplicito consenso dell'insegnante e quindi per scopi che non siano didattici;
   c. giocare con i dispositivi.

10. Diritto di ispezione degli Insegnanti: la scuola si riserva il diritto di monitorare le attività online degli utenti e accedere, controllare, copiare, raccogliere o cancellare ogni comunicazione elettronica o file, rivelandone il contenuto alle forze dell'ordine qualora lo ritenga necessario.

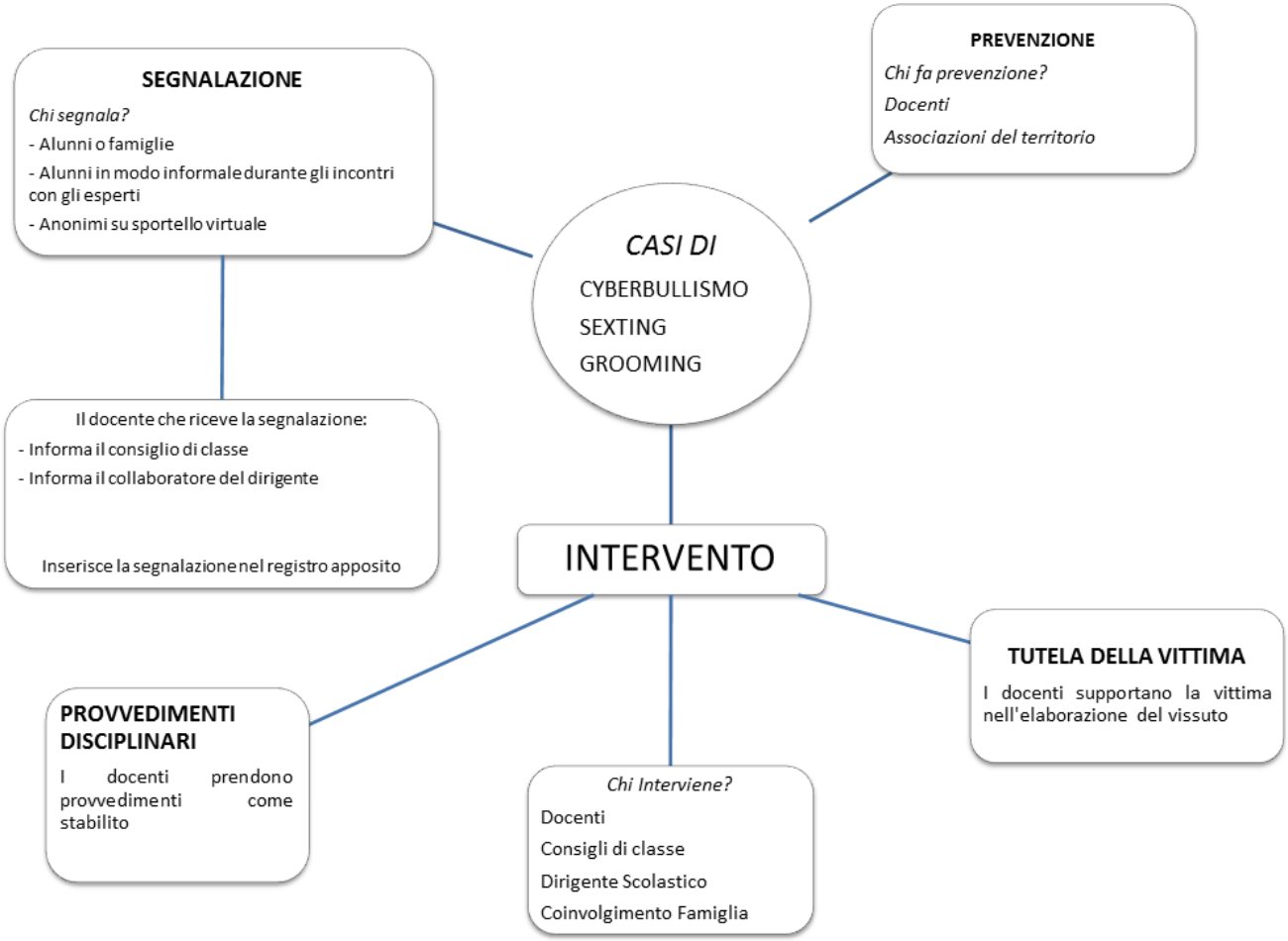
- ***Per i docenti***

1. I Docenti sono responsabili del proprio dispositivo: questi non possono essere lasciati incustoditi, se accesi, e non posso essere prestati agli alunni.
2. Sono ammessi in classe per soli fini didattici: computer portatili, tablet, smartphone, e-reader, ecc...
3. I docenti possono usare dispositivi di registrazione audio, video, foto (o dispositivi che li prevedano) a fini didattici. La diffusione del materiale potrà avvenire previa autorizzazione scritta delle famiglie.
4. Ai docenti non è consentito usare Internet per scopi diversi da quelli didattici;
5. Diritto di ispezione del Dirigente Scolastico, o di persona da esso delegata: la scuola si riserva il diritto di monitorare le attività online degli utenti che utilizzano la rete Wifi della scuola e controllare ogni comunicazione elettronica, rivelandone il contenuto alle forze dell'ordine qualora lo ritenga necessario.
6. L'uso improprio verrà sanzionato in base alla normativa vigente.

- ***Per i collaboratori scolastici***

Fatti salvi i momenti di pausa, ai collaboratori scolastici non è consentito in alcun modo l'uso di strumenti tecnologici personali (pc portatili, tablet, smartphone, e-reader, cellulari….). L'uso improprio verrà sanzionato in base alla normativa vigente.

5. Prevenzione, rilevazione e gestione dei casi



Prevenzione:

I docenti svolgeranno attività di formazione/informazione in classe adeguando le attività all'età degli alunni e avvalendosi di materiali di supporto, fra cui anche quelli messi a disposizione da "Generazioni Connesse". La prevenzione passa poi anche attraverso percorsi di educazione all'affettività e all'emotività che già si svolgono in istituto. In collaborazione con associazioni del territorio si attueranno anche attività di sensibilizzazione alle famiglie.

In particolare le attività si concentreranno sull'analisi dei rischi in rete maggiormente diffusi:

- Cyberbullismo.
- Sexiting.
- Grooming.

Azioni:

Le azioni d'intervento del personale scolastico andranno ad agire su più piani:

1. Rilevazione

Le azioni verranno intraprese a seguito di:

- segnalazioni da parte degli alunni o delle famiglie
- segnalazioni durante gli incontri con gli esperti
- segnalazioni su sportello virtuale

2. Segnalazione

Il docente che riceve la segnalazione deve provvedere a informare il consiglio di classe e il collaboratore del dirigente che provvederà ad inserire la segnalazione nel registro apposito

2. Gestione dei casi

Il Dirigente scolastico e/o il Consiglio di classe ha la possibilità di sostituire le sanzioni disciplinari più severe con altri provvedimenti, comprendenti la collaborazione ai servizi interni della scuola o altre attività a scopo sociale che possono utilmente costituire una riparazione ed un ammonimento, quali:

- cooperazioni di pulizia e ripristino degli arredi dei locali scolastici;
- collaborazione con il personale ausiliario;
- riordino della biblioteca e/ o dei laboratori;
- ricerche e/o attività di studio ed approfondimento coerenti con l'infrazione commessa

EPISODIO SEGNALATO	**ISTIGATORE**		**VITTIMA**	
	Frequenza	Provvedimento	Organo	Intervento
Cyberbullismo				
Comportamenti verbali deliberatamente ostili e provocatori nei confronti di compagni, insegnanti e personale non docente: l'invio di messaggi elettronici, violenti e volgari allo scopo di suscitare conflitti verbali.	1° volta 2° volta Ulteriori episodi	○ Richiamo verbale ○ Ammonizione scritta sul diario ○ Ammonizione scritta sul diario e sul registro ○ Sospensione dalle visite guidate, viaggi d'istruzione, gruppi sportivi ed altre attività con obbligo della presenza a scuola ○ Abbassamento del voto condotta ○ Diffida scritta con comunicazione alla famiglia da parte del Dirigente Scolastico	Docente Consiglio di classe	*I docenti:* • colloquio individuale con la vittima ed eventuale orientamento allo sportello di ascolto; • sensibilizzazione e coinvolgimento del gruppo classe per supportare le difficoltà; • informazione e coinvolgimento della famiglia. *Il Dirigente Scolastico*: In caso di reiterazione di atti nei confronti della stessa vittima, deciderà se il fatto vada riportato alle autorità di competenza.

Fatti gravi o parole che consapevolmente tendono ad emarginare gli altri studenti: ***Harassment*** Molestie persistenti e ripetute, dirette verso una persona specifica, che possono causare disagio emotivo e psichico. ***Cyberstalking*** Comportamenti che, attraverso l'uso delle nuove tecnologie, sono finalizzati a perseguitare le vittime in diversi modi e hanno lo scopo di infastidirle e molestarle, sino a commettere atti di aggressione molto più violenti, anche di tipo fisico. ***Denigration*** Distribuzione, all'interno della rete o tramite SMS, di messaggi falsi o dispregiativi nei confronti delle vittime, con lo scopo "di danneggiare la reputazione o le amicizie di colui che viene preso di mira". ***Exclusion*** Esclusione intenzionale di un pari dal proprio gruppo di amici, dalla chat o da un gioco interattivo.		○ Richiamo verbale. ○ Sequestro strumento. ○ Rimozione dalla rete del materiale causa di molestie. ○ Ammonizione sul diario e sul registro ○ Comunicazione dell'avvenuto alla famiglia, attuazione interventi in collaborazione con la famiglia (eventuale impedimento di accesso alla rete). ○ Eventuale sospensione dell´intervallo o di altri servizi. ○ Abbassamento voto di condotta. ○ Diffida scritta con comunicazione alla famiglia da parte del Dirigente Scolastico. ○ Sospensione con attività educative da svolgere in collaborazione con la famiglia.		
Sexting Invio e condivisione di testi o immagini sessualmente esplicite tramite internet o telefono cellulare **Grooming** Adescamento di un minore in internet tramite manipolazione psicologica volta a superarne le resistenze, a ottenerne la fiducia e abusarne sessualmente	In caso di segnalazione, gli episodi di *sexting o grooming* verranno valutati singolarmente e - previo coinvolgimento della famiglia - si stabilirà la modalità d'intervento e l'eventuale comunicazione agli organi competenti.			