

Documento di ePolicy

VIIC872001

IC VICENZA 2 - VIA PIOVENE

VIA PIOVENE 31 - 36100 - VICENZA - VICENZA (VI)

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

Le TIC (Tecnologie dell'informazione e della comunicazione) rappresentano strumenti fondamentali nel processo educativo e per l'apprendimento degli studenti e delle studentesse.

Le "competenze digitali" sono fra le abilità chiave all'interno del [Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente](#) e di esse bisogna dotarsi proprio a partire dalla scuola (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

In un contesto sempre più complesso, diventa quindi essenziale per ogni Istituto Scolastico dotarsi di una E-policy, un documento programmatico volto a promuovere le competenze digitali ed un uso delle tecnologie positivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che degli adulti coinvolti nel processo educativo. L'E-policy, inoltre, vuole essere un documento finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti.

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Argomenti del Documento

1. Presentazione dell'ePolicy

1. Scopo dell'ePolicy
2. Ruoli e responsabilità
3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

5. Gestione delle infrazioni alla ePolicy
6. Integrazione dell'ePolicy con regolamenti esistenti
7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento

2. Formazione e curriculum

1. Curriculum sulle competenze digitali per gli studenti
2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
4. Sensibilizzazione delle famiglie e Patto di corresponsabilità

3. Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola

1. Protezione dei dati personali
2. Accesso ad Internet
3. Strumenti di comunicazione online
4. Strumentazione personale

4. Rischi on line: conoscere, prevenire e rilevare

1. Sensibilizzazione e prevenzione
2. Cyberbullismo: che cos'è e come prevenirlo
3. Hate speech: che cos'è e come prevenirlo
4. Dipendenza da Internet e gioco online
5. Sexting
6. Adescamento online
7. Pedopornografia

5. Segnalazione e gestione dei casi

1. Cosa segnalare
2. Come segnalare: quali strumenti e a chi
3. Gli attori sul territorio per intervenire
4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

La comunità scolastica ha un ruolo fondamentale nel garantire che bambini e ragazzi siano in grado di utilizzare le tecnologie digitali e la Rete e di farlo in modo appropriato, responsabile e sicuro.

Questo documento è stato elaborato seguendo le LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo (elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con "Generazioni Connesse" e il Safer Internet Center per l'Italia, programma comunitario istituito dal DF C Europeo e dal Consiglio dell'Unione) e le LINEE GUIDA per l'uso positivo delle tecnologie digitali e la prevenzione dei rischi nelle scuole, sempre nell'ambito di Generazioni Connesse.

Il documento vuole coinvolgere tutte le componenti della Comunità scolastica per delineare l'insieme di Regolamenti, Linee di azione e attività che determinano la condotta da porre in essere per facilitare e promuovere l'utilizzo delle Tecnologie dell'Informazione e della Comunicazione (da qui TIC) nella didattica e per determinare le azioni di prevenzione rispetto ai rischi del navigare in Rete, nonché le misure di gestione di situazioni problematiche.

La nostra vision e mission in merito alle TIC riguarda:

- l'approccio educativo alle tematiche connesse alle "competenze digitali", alla privacy, alla sicurezza online e all'uso delle tecnologie digitali nella didattica e nel percorso educativo;
- le norme comportamentali e le procedure di utilizzo delle Tecnologie dell'Informazione e della Comunicazione (ICT) in ambiente scolastico;
- le misure per la prevenzione e la sensibilizzazione di comportamenti on-line a rischio;
- le misure per la rilevazione, segnalazione e gestione delle situazioni rischiose legate ad un uso non corretto delle tecnologie digitali.

Il Documento

1. Presentazione dell'ePolicy
 1. Scopo dell'ePolicy
 2. Ruoli e responsabilità
 3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
 4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
 5. Gestione delle infrazioni alla ePolicy
 6. Integrazione dell'ePolicy con regolamenti esistenti
 7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. Formazione e curriculum
 1. Curriculum sulle competenze digitali per gli studenti
 2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
 3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
 4. Sensibilizzazione delle famiglie e Patto di corresponsabilità

3. Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola
 1. Protezione dei dati personali
 2. Accesso ad Internet
 3. Strumenti di comunicazione online
 4. Strumentazione personale
4. Rischi on line: conoscere, prevenire e rilevare
 1. Sensibilizzazione e prevenzione
 2. Cyberbullismo: che cos'è e come prevenirlo
 3. Hate speech: che cos'è e come prevenirlo
 4. Dipendenza da Internet e gioco online
 5. Sexting
 6. Adescamento online
 7. Pedopornografia
5. Segnalazione e gestione dei casi
 1. Cosa segnalare
 2. Come segnalare: quali strumenti e a chi
 3. Gli attori sul territorio per intervenire
 4. Allegati con le procedure

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

1.2 - Ruoli e responsabilità

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ognuno, secondo il proprio ruolo, s'impegni nell'attuazione e promozione di essa.

Dirigente Scolastico:

Prof. Alfonso Sforza

- **garantisce una formazione adeguata del Personale Scolastico;**
- **garantisce la tutela legale riguardante la Privacy e la tutela dell'immagine dei membri della Comunità Scolastica;**

- **garantisce l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on line;**
- **supporta il Personale Scolastico nelle procedure per la segnalazione e gestione dei casi che dovessero verificarsi.**

Direttore dei Servizi Generali ed Amministrativi:

- **assicura, nei limiti delle risorse finanziarie disponibili gli interventi di manutenzioni richieste da un cattivo funzionamento e o danneggiamento della dotazione tecnologica dell'istituto.**
- **cura la registrazione dei disservizi e delle problematiche relative alla rete, segnalati dai docenti, provvedendo all'intervento del Personale di Assistenza**

Referenti bullismo e cyberbullismo:

- **coordinano e promuovono iniziative specifiche per la prevenzione ed il contrasto del bullismo e del cyberbullismo;**
- **coinvolgono studenti, colleghi e genitori in progetti e percorsi formativi.**

Animatore Digitale e Team Digitale:

- **individua soluzioni tecnologiche, coerente con l'analisi dei fabbisogni dell'Istituto, anche in sinergia con attività di assistenza tecnica condotta da altre figure;**
- **monitora e rileva le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di Internet a scuola;**
- **favorisce la formazione interna per lo sviluppo della "scuola digitale" e della sicurezza in rete**

Docenti:

- **provvedono alla propria formazione sull'utilizzo del digitale con particolare riferimento alla dimensione etica: tutela della Privacy, rispetto dei diritti d'autore dei materiali reperiti in Internet, lotta al cyberbullismo;**
- **sviluppano le competenze digitali degli alunni;**
- **fanno in modo che gli alunni conoscano e rispettino le norme di sicurezza nell'uso del web ed utilizzino correttamente le tecnologie digitali;**
- **comunicano ai genitori difficoltà, bisogni o disagi espressi dagli alunni rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;**
- **segnalano al Dirigente Scolastico e al team per il contrasto al bullismo/cyberbullismo eventuali episodi di violazione delle norme di comportamento stabilite.**

Personale Amministrativo, Tecnico e Ausiliario (ATA):

- **è coinvolto attivamente nell'applicazione delle legge 107/15 ("La Buona Scuola") che concerne non solo il tempo scuola e l'ampliamento dell'offerta formativa, ma anche le attività di formazione ed autoformazione sui temi del bullismo/cyberbullismo**
- **è coinvolto nella formazione per il rispetto e la tutela dei dati sensibili;**
- **è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo**

Alunni:

tenendo conto del grado di maturità e di apprendimento

- **rispettano le norme di sicurezza nell'uso del web ed utilizzano correttamente le tecnologie digitali;**

conoscono le buone pratiche di sicurezza on-line

- **adottano condotte rispettose degli altri durante la comunicazione in Rete;**
- **chiedono l'intervento dell'insegnante e/o dei genitori qualora insorgano difficoltà/dubbi durante l'utilizzo dei mezzi digitali**

Genitori:

- **contribuiscono, in sinergia con la scuola, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;**
- **agiscono in modo coerente alle finalità dell'E-policy dell'Istituto, sia per la prevenzione dei rischi, sia per l'attuazione delle procedure previste in caso di violazione delle regole stabilite;**
- **monitorano l'uso di Internet e dei vari dispositivi da parte dei figli**

1.3 - Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio di interesse superiore del minore, ascoltare e prendere in seria considerazione le opinioni ed i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa.

Sono vietati i comportamenti irrispettosi, offensivi o lesivi della privacy, dell'intimità e degli spazi personali degli studenti e delle studentesse oltre che quelli legati a tollerare o partecipare a comportamenti di minori che sono illegali, o abusivi o che mettano a rischio la loro sicurezza.

Tutti gli attori esterni sono tenuti a conoscere e rispettare le regole del nostro Istituto dove sono esplicitate le modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e quelli in dotazione della scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse. Esiste l'obbligo di rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti

personali (numero, mail, chat, profili di social network).

Al fine della massima tutela degli studenti, anche i soggetti esterni che erogano attività nell'Istituto sono tenuti a prendere visione dei documenti che regolano l'uso dei propri dispositivi personali e quelli in dotazione della scuola e che sanciscono l'obbligo del rispetto della privacy (soprattutto degli alunni minorenni) e a sottoscriverli preliminarmente all'avvio degli interventi con gli alunni, in classe o fuori.

I soggetti esterni, prima dell'intervento in classe, devono prendere visione dell'informativa e sottoscriverla, inserendo i loro dati personali, il progetto specifico, le attività previste con gli alunni e i nominativi del Docente di riferimento. L'informativa viene condivisa e sottoscritta nella stipula dei contratti con personale ed associazioni esterne. A maggior tutela dei minori l'Istituto chiede agli attori esterni di produrre il certificato penale per accertarsi che il soggetto da impiegare non sia stato già condannato per reati contro i minori (prostituzione minorile, pornografia minorile, pornografia virtuale, turismo sessuale e adescamento dei minorenni - in attesa del documento, si potrà accettare un'autocertificazione sostitutiva in cui il lavoratore dichiara di non essere stato condannato per i reati contro i minori).

1.4 - Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica

Il documento di E-policy viene condiviso con tutta la comunità educante, ponendo al centro gli studenti e le studentesse e sottolineando compiti, funzioni e attività reciproche. È molto importante che ciascun attore scolastico (dai docenti agli/lle studenti/esse) si faccia a sua volta promotore del documento.

L'E-policy viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:

- la pubblicazione del documento sul sito istituzionale della scuola;
- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line, negli spazi della scuola e sulle regole di condotta da tenere in Rete.

L'E-policy viene presentata al Collegio Docenti per l'approvazione e quindi al Consiglio d'Istituto per la delibera; viene quindi pubblicata nel sito www.icvicenza2.edu.it.

Condividere e comunicare le linee di sicurezza agli alunni

Nell'informazione/educazione in merito alla sicurezza, è data particolare attenzione agli aspetti nei quali gli alunni risultano più vulnerabili.

- **Gli alunni sono informati che l'uso di Internet e di ogni dispositivo digitale è controllato dagli insegnanti e che dev'essere utilizzato solo con la loro autorizzazione.**
- **L'istruzione degli alunni riguardo all'uso responsabile e sicuro di Internet precede l'accesso alla rete.**
- **L'elenco delle regole per la sicurezza on-line è esposto in tutte le aule o laboratori con accesso a Internet.**
- **I Coordinatori di classe all'inizio dell'anno scolastico prevedono dei momenti di discussione e condivisione con gli alunni del Patto di Corresponsabilità che comprende anche l'utilizzo consapevole delle TIC e della Rete. Per sensibilizzare anche gli alunni più piccoli della Scuola Primaria si utilizzano materiali, mezzi e strumenti adeguati.**

Condividere e comunicare le linee di sicurezza ai genitori

È auspicabile, al fine della tutela dell'alunno, un rapporto di condivisione e collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di Internet in occasione degli incontri scuola-famiglia, collegiali e individuali.

- **L'Animatore Digitale fornisce ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di Internet, anche a casa.**
- **L'Animatore Digitale e i docenti di classe forniscono ai genitori indirizzi sul web relativi a risorse utili per lo studio e a sistemi di controllo.**

Durante le assemblee con i genitori, i coordinatori di classe presentano i punti salienti del documento e chiedono ai genitori di sottoscrivere il Patto di Corresponsabilità (integrato con la voce riguardante il documento E-policy).

Condividere e comunicare le linee di sicurezza al personale

La linea di condotta dell'Istituto in materia di sicurezza nell'utilizzo delle tecnologie digitali e di Internet è oggetto di discussione negli Organi Collegiali e comunicata formalmente a tutto il Personale con il presente documento e altro materiale informativo anche sul sito web.

- Una idonea informazione-formazione on line sull'uso sicuro e responsabile di Internet, compatibile con il ruolo professionale, è fornita a tutto il personale docente, anche attraverso il sito web della scuola.**
 - Una idonea informazione-formazione on line sul trattamento dei dati particolari e dei dati personali (in conformità al Regolamento Generale per la Protezione dei Dati) è fornita a tutto il personale, anche attraverso il sito web della scuola.**
 - Il monitoraggio sull'utilizzo delle TIC è supervisionato dall'Animatore Digitale che segnala al Dirigente Scolastico e al Direttore dei Servizi Generali e Amministrativi eventuali problemi che dovessero richiedere acquisti o interventi di tecnici.**
 - L'Animatore Digitale evidenzia strumenti utili che il personale docente può utilizzare per lo sviluppo di una didattica digitale.**
 - Il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e con i propri doveri professionali è sanzionabile.**
-

1.5 - Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all'E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di eventuali violazioni

Gestione delle infrazioni all'E-policy: condotte sanzionabili, in relazione all'uso improprio delle TIC e della Rete a Scuola da parte degli alunni.

Perchè la Scuola è chiamata ad intervenire nelle questioni di emergenza/gestione delle infrazioni?

- per porre fine al disagio/sofferenza della vittima
- per responsabilizzare il bullo/i rispetto all'azione
- per dare un chiaro messaggio a tutti gli alunni che atti di bullismo/cyberbullismo non vengono accettati nella scuola
- per dimostrare ai genitori delle vittime, e a tutti i genitori in generale, che la scuola risponde prontamente a simili emergenze/infrazioni

Le eventuali infrazioni in cui è possibile che gli *alunni* incorrano nell'utilizzo delle tecnologie digitali di Internet di cui si dispone per la didattica possono essere le seguenti:

- l'invio avventato o senza permesso di foto o di altri dati personali
- la condivisione di immagini non adeguate o che ledono terzi
- la comunicazione imprudente, non autorizzata, con sconosciuti
- il collegamento a siti web non indicati dai docenti

In che modo la Scuola è chiamata ad intervenire nelle questioni di emergenza/gestione delle infrazioni?

La scuola ha un Team per la gestione dei casi, in stretta connessione con i Servizi del Territorio per le situazioni più gravi, ed è dotata di un Protocollo di azione, che prevede una fase di prima segnalazione, una seconda di valutazione e di approfondimento con i soggetti coinvolti nel caso, una terza fase di scelta dell'intervento e della gestione del caso e un'ultima fase di monitoraggio.

Proprio in merito alla gestione del caso, in base alla gravità, si procede con interventi diversi:

- un approccio educativo con la classe;

- un intervento individuale;
- una gestione della relazione;
- il coinvolgimento della famiglia;
- un supporto intensivo a lungo termine e di rete.

A seconda dell'età dell'alunno è importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione allo scopo di promuovere una maggior consapevolezza sull'utilizzo di Internet.

La violazione delle norme previste nel REGOLAMENTO SULL'USO DI DISPOSITIVI ELETTRONICI DA PARTE DEGLI ALUNNI comporta l'irrogazione di sanzioni disciplinari, secondo quanto previsto dal Regolamento di Disciplina. Nei casi più gravi potrebbero anche configurarsi situazioni per le quali è necessario l'intervento della Polizia Postale e/o dei Servizi preposti.

Le eventuali infrazioni in cui è possibile che i *docenti* incorrano nell'utilizzo delle tecnologie digitali di Internet di cui si dispone per la didattica possono essere le seguenti:

- utilizzo delle tecnologie e dei servizi della scuola non legato alle attività di insegnamento
- custodia non adeguata delle password assegnate
- comunicazioni, attraverso gli strumenti digitali, con genitori e alunni non riferibili al ruolo
- trattamento dei dati personali degli alunni non conforme al GDPR
- insufficiente informazione agli alunni sull'utilizzazione responsabile delle tecnologie digitali e di Internet
- insufficiente vigilanza degli alunni che può causare da parte di qualcuno di essi un utilizzo inadeguato delle TIC, lesivo per se stesso o per gli altri
- nelle questioni di emergenza, segnalazioni inadeguate o non tempestive a chi di competenza (Dirigente Scolastico, Team preposto)

In che modo la Scuola è chiamata ad intervenire nelle questioni di emergenza/gestione delle infrazioni?

Il Dirigente Scolastico può controllare l'utilizzo delle TIC per appurarne la conformità. L'avvio di procedimenti di vario carattere, in base al tipo di infrazione, segue le procedure stabilite dalle vigenti normative e dal Contratto Collettivo Nazionale di Lavoro.

Per garantire sempre più una fruizione corretta delle TIC ed una navigazione responsabile in Internet, al fine di arginare il veicolarsi a scuola di materiale reperito in contesti extrascolastici, si raccomanda alle famiglie di accompagnare i propri figli nella navigazione in Rete e nell'utilizzo del cellulare, vigilando attentamente nel caso di una fruizione in autonomia concessa al proprio figlio.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

L'E-policy, in conformità con le vigenti normative, va ad integrarsi con gli obiettivi del PTOF, con il Regolamento di Istituto, con il Regolamento sull'uso dei dispositivi elettronici e con il Patto di Corresponsabilità.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

L'E-policy viene aggiornata periodicamente e quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola. Le modifiche del documento saranno discusse con tutti i membri del personale docente. Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

Il monitoraggio dell'E-policy è svolto annualmente dal Dirigente Scolastico con la collaborazione dell'Animatore Digitale e del Team E-policy.

Esso è finalizzato:

- alla rilevazione della situazione iniziale e di quella finale delle classi in merito ad un uso corretto delle TIC e ad una responsabile navigazione in Rete;

- alla valutazione dell'efficacia dell'E-policy;

- alla rilevazione dei nuovi bisogni emersi nel corso dell'anno scolastico, anche sulla base dei dati raccolti:

- ANNO SCOLASTICO
- NUMERO DI SEGNALAZIONI
- NUMERO DI INFRAZIONI
- NUMERO DI SANZIONI DISCIPLINARI

L'aggiornamento della E-policy, sulla base di quanto rilevato nella fase di monitoraggio, è curato dal Dirigente Scolastico, dall'Animatore Digitale, dagli Organi Collegiali.

Capitolo 2 - Formazione e curriculum

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più “intuitivo” ed “agile” rispetto agli adulti, ma non per questo sono dotati di maggiori “competenze digitali”.

Infatti, “la competenza digitale presuppone l’interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l’alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l’alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l’essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico” ([“Raccomandazione del Consiglio europeo relativa alla competenze chiave per l’apprendimento permanente”, C189/9, p.9](#)).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curriculum digitale.

“La competenza digitale presuppone l’interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l’alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l’alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l’essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico.” (Nuove Raccomandazioni europee, 2018)

In riferimento alle *Conoscenze, abilità e atteggiamenti essenziali legati a tale competenza* le Nuove Raccomandazioni aggiungono:

“Le persone dovrebbero comprendere in che modo le tecnologie digitali possono essere di aiuto alla comunicazione, alla creatività e all’innovazione, pur nella consapevolezza di quanto ne consegue in termini di opportunità, limiti, effetti e rischi. [...] Le abilità comprendono la capacità di utilizzare, accedere a, filtrare, valutare, creare, programmare e condividere contenuti digitali. Le persone dovrebbero essere in grado di gestire e proteggere informazioni, contenuti, dati e identità digitali,

oltre a riconoscere software, dispositivi, intelligenza artificiale o robot e interagire efficacemente con essi.

Interagire con tecnologie e contenuti digitali presuppone un atteggiamento riflessivo e critico, ma anche improntato alla curiosità, aperto e interessato al futuro della loro evoluzione. Impone anche un approccio etico, sicuro e responsabile all'utilizzo di tali strumenti."

"La responsabilità è l'atteggiamento che connota la competenza digitale. Solo in minima parte essa è alimentata dalle conoscenze e dalle abilità tecniche, che pure bisogna insegnare. I nostri ragazzi, anche se definiti nativi digitali, spesso non sanno usare le macchine, utilizzare i software fondamentali, fogli di calcolo, elaboratori di testo, navigare in rete per cercare informazioni in modo consapevole. Sono tutte abilità che vanno insegnate. Tuttavia, come suggeriscono anche i documenti europei sulla educazione digitale, le abilità tecniche non bastano. La maggior parte della competenza è costituita dal sapere cercare, scegliere, valutare le informazioni in rete e nella responsabilità nell'uso dei mezzi, per non nuocere a se stessi e agli altri". (Indicazioni Nazionali e nuovi scenari, 2017).

Accanto alle altre Competenze trasversali, il Documento annovera le competenze digitali tra le Competenze Chiave irrinunciabili per le quali i Curricoli "dovrebbero prevedere precisi riferimenti in termini di risultati di apprendimento, evidenze, percorsi didattici, criteri di valutazione. [...] Senza queste competenze non sono possibili né una corretta e proficua convivenza né un accesso consapevole e critico alle informazioni né si hanno gli strumenti per affrontare e risolvere problemi, prendere decisioni, pianificare e progettare, intervenire sulla realtà e modificarla".

In tutte le discipline sono presenti abilità e conoscenze riconducibili alle competenze digitali e tutte concorrono a costruirle. Ed è in questo senso che tutti gli insegnanti sono coinvolti in tale costruzione.

Il nostro Istituto condivide le linee indicate nel Piano Nazionale Scuola Digitale (PNSD) . Esse danno come indirizzo l'intento di migliorare gli ambienti di apprendimento per rendere l'offerta formativa rispondente *alle sfide di un mondo che cambia rapidamente, che richiede sempre di più agilità mentale, competenze trasversali e un ruolo attivo dei giovani*, che hanno esigenze e stili cognitivi diversi dalle generazioni non digitali.

Il D.M. 851 del 27 ottobre 2015 ne prevede l'attuazione in conformità all'art.1, comma 58 della Legge 107/2015 che dispone di:

- realizzare attività volte allo sviluppo delle competenze digitali degli studenti;
- potenziare le dotazioni tecnologiche della scuola al fine di migliorare gli strumenti didattici e laboratoriali presenti;
- favorire la formazione dei docenti per l'innovazione didattica e sviluppo della cultura digitale per l'insegnamento, l'apprendimento e la formazione delle competenze lavorative, cognitive e sociali degli studenti;
- potenziare le infrastrutture di rete.
- individuare un Animatore Digitale ed un Team per l'innovazione digitale che supporti ed accompagni adeguatamente l'innovazione didattica, nonché l'attività dell'animatore Digitale;
- partecipare a bandi nazionali ed europei per finanziare le suddette iniziative.

<https://icvicenza2.edu.it/wp-content/uploads/sites/131/COMPETENZE-DIGITALI.pdf>

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

I docenti hanno partecipato a corsi di formazione nell'ambito di Piani Nazionali oltre che ad iniziative interne all'Istituto - secondo un piano voluto dal Dirigente Scolastico rispondente alle necessità emerse dopo l'analisi dei bisogni - o programmate dall'Ambito 8 - Vicenza città e area Berica, di cui il nostro Istituto fa parte.

Tutti i docenti possiedono una buona base di competenze e nel caso di Figure di sistema, anche di carattere specialistico.

Il percorso della formazione dei docenti sull'utilizzo delle TIC nella didattica non può ritenersi esaurito nell'arco di un anno scolastico, pertanto anche per i prossimi anni, oltre a percorsi di formazione personale, on line o in presenza, sono previste iniziative di formazione collettiva all'interno dell'Istituto, di partecipazione a corsi promossi dall'Amministrazione centrale e dalle Scuole Polo per la Formazione.

I docenti, inoltre, possono sempre fruire del materiale messo a disposizione dall'Animatore Digitale.

L'I.C. Vicenza 2 dall'anno 2019/2020 ha attivato in tutte le classi della Scuola dell'Infanzia, della Scuola Primaria e della Scuola Secondaria di I grado la *GSuite for Education*: piattaforma per uso interno e protetto (non profilato e con spazio a disposizione illimitato) dove è possibile scambiarsi materiale e condividere lavori sia tra docenti sia con gli alunni, attraverso numerose applicazioni tra cui la Google Classroom.

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

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che, con cadenza, verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

La Scuola è chiamata a mettere in atto percorsi di Prevenzione Universale che mirano alla riduzione del rischio e alla promozione delle risorse e della resilienza. Per questo adotta un approccio sistemico rivolto a tutta la comunità scolastica.

La centralità del ruolo dell'insegnante impone una formazione atta a:

- conoscere per prevenire;
- conoscere per acquisire consapevolezza, per essere maggiormente supportivi;
- conoscere per formare, a loro volta, gli alunni, per renderli fruitori consapevolmente responsabili.

La formazione dei Docenti vuole, in tal senso, approfondire gli aspetti legati alle attività da fare con gli alunni, cercando di fornire indicazioni teoriche, tipologie di stimoli, spunti operativi su come organizzare e strutturare un percorso di prevenzione universale, all'interno di un più vasto percorso che è quello curricolare.

A momenti di formazione personale o collettiva, legata alla veloce evoluzione delle tecnologie e delle modalità di comunicazione, di cui i ragazzi sono sempre più fruitori autonomi, l'Istituto predispone una apposita bacheca sul sito istituzionale per la messa a disposizione di:

- materiali per l'aggiornamento sulla sicurezza in Internet per l'approfondimento personale, per le attività con gli alunni e gli incontri con i genitori, costituiti da slide, testi e link a siti specializzati forniti dalla Piattaforma Elisa al Team Bullismo e Cyberbullismo;
- contributi derivanti dal Safer Internet Centre – Generazioni Connesse, Progetto coordinato dal MIUR con il partenariato di alcune delle principali realtà italiane che si occupano di sicurezza in Rete (Autorità Garante per l'Infanzia e l'Adolescenza, Polizia di Stato, Telefono Azzurro, Skuola net ...) con l'obiettivo di "fornire informazioni e supporto ad alunni, genitori, docenti ed educatori che hanno esperienze, anche problematiche, legate a Internet e per agevolare la segnalazione di materiale illegale online".

L'I.C. 2 ha organizzato per i docenti della Scuola Secondaria di I grado un incontro sull'utilizzo consapevole di e sicuro di Internet, come misura di prevenzione al cyberbullismo; si prevede di allargare questo momento di informazione/formazione alle docenti delle Scuole Primarie, visto il

precoce utilizzo autonomo dei dispositivi digitali.

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali, anche in una prospettiva lavorativa futura. L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy e dal suo piano di azioni, anche attraverso l'aggiornamento, oltre che del regolamento scolastico, anche del "Patto di corresponsabilità" e attraverso una sezione dedicata sul sito web dell'Istituto.

La Scuola, cosciente che, nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti (ognuno secondo i propri ruoli e le proprie responsabilità), promuove iniziative per la condivisione con le famiglie di un percorso educativo teso ad un uso responsabile e proficuo delle tecnologie digitali da parte dei bambini e dei ragazzi.

A tal fine sono previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate, messo a disposizione dai siti specializzati e dalle Forze dell'Ordine.

Si prevede anche di organizzare un incontro con gli alunni della Scuola Secondaria con l'intervento degli operatori della Polizia Postale e delle Forze dell'Ordine.

Sono favoriti momenti di informazione/confronto/discussione anche sulle dinamiche che potrebbero instaurarsi fra gli alunni con l'uso di cellulari, smartphone, chat, social network, con particolare riferimento alla prevenzione del cyberbullismo.

I materiali di approfondimento (quali guide, video...), rivolti agli alunni e ai tutori sono raccolti sul sito dell'Istituto.

La scuola si impegna alla diffusione delle informazioni e delle procedure incluse nel presente documento per portare a conoscenza delle famiglie il Regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e prevenire i rischi legati a un utilizzo non corretto della Rete.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023)

Promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

Organizzare incontri con esperti e/o forze dell'ordine per i genitori sull'educazione alla cittadinanza digitale.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi)

Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.

Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.

Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

Organizzare incontri con esperti per i docenti sulle competenze digitali.

Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

Capitolo 3 - Gestione dell'infrastruttura e della strumentazione ICT della e nella scuola

3.1 - Protezione dei dati personali

“Le scuole sono chiamate ogni giorno ad affrontare la sfida più difficile, quella di educare le nuove generazioni non solo alla conoscenza di nozioni basilari e alla trasmissione del sapere, ma soprattutto al rispetto dei valori fondanti di una società. Nell'era di Internet e in presenza di nuove forme di comunicazione questo compito diventa ancora più cruciale. È importante riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino”.

(cfr. <http://www.garanteprivacy.it/scuola>).

Ogni giorno a scuola vengono trattati numerosi dati personali sugli studenti e sulle loro famiglie. Talvolta, tali dati possono riguardare informazioni sensibili, come problemi sanitari o particolari disagi sociali. Il “corretto trattamento dei dati personali” a scuola è condizione necessaria per il rispetto della dignità delle persone, della loro identità e del loro diritto alla riservatezza. Per questo è importante che le istituzioni scolastiche, durante lo svolgimento dei loro compiti, rispettino la privacy, tutelando i dati personali dei soggetti coinvolti, in particolar modo quando questi sono minorenni.

La protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8), tutelato dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

Anche le scuole, quindi, hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101, entrato in vigore lo scorso 19 settembre.

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare riferimento all'uso delle tecnologie digitali, e indichiamo le misure che la scuola intende attuare per garantire la tutela della privacy e il diritto alla riservatezza di tutti i soggetti coinvolti nel processo educativo, con particolare attenzione ai minori. A tal fine, l'Istituto allega alla presente ePolicy i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati

personali.

LEGGI DI RIFERIMENTO

Riguardo ai principi generali cui attenersi in termini di etica e di buon uso dei servizi in rete, l'I.C. 2 prende come riferimento i principi proposti dal MIUR nel documento *“La posizione italiana sui principi fondamentali di Internet”*, 2012 in cui i principi fondanti della rete sono suddivisi in cinque sezioni che identificano gli ambiti cui si riferiscono:

- a. Principi generali: Internet bene comune;
- b. Cittadinanza in Rete;
- c. Consumatori e utenti della Rete;
- d. Produzione e circolazione dei contenuti;
- e. Sicurezza in rete.

Il Personale Scolastico è “incaricato del trattamento” dei dati personali (degli Alunni, dei Tutori, del Personale), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della Docenza (istruzione e formazione).

Tutto il Personale incaricato riceve Istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.

Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni, eccedenti i trattamenti istituzionali obbligatori.

A tal fine, si allega il link dell'Informativa per i genitori conforme alla normativa vigente, in materia di protezione dei dati personali.

https://icvicenza2.edu.it/wp-content/uploads/sites/131/firmato_1578497753_GDPR_-_Informativa_Genitori_e_Alunni.pdf

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti*

sostanziali e non solo come possibilità di collegamento alla Rete.

- 4. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
- 5. Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

ACCESSO AD INTERNET: FILTRI, ANTIVIRUS E SULLA NAVIGAZIONE

L'accesso a Internet è possibile e consentito per la didattica in tutti i plessi delle Scuole dell'Infanzia, Primaria e della Secondaria di 1° grado, attraverso reti LAN e Wi-Fi; le credenziali del Wi-Fi non sono fornite agli alunni, ma sono comunicate a tutti i docenti e memorizzate nei device dell'I.C.2.

Le attività sulle postazioni fisse nei Laboratori e nelle LIM sono vigilate e mediate dai Docenti.

I Docenti registrano/prenotano il proprio accesso al Laboratorio, scrivendo su un registro la data e l'orario di utilizzo; gli alunni firmano la presenza in un file dedicato e caricano i propri materiali in una apposita cartella (o nella propria chiavetta USB).

I responsabili delle Aule d'Informatica periodicamente provvedono alla manutenzione e all'aggiornamento del sistema, richiedendo, ove necessario, l'intervento di tecnici esterni.

La posta elettronica istituzionale (fornita ad ogni Docente e al Personale ATA) è protetta da antispyware, ed è fornita da Google for Education.

Si sensibilizza la Comunità scolastica sull'opportunità di tenere aggiornati gli antivirus installati sui

device personali e di controllare i dispositivi di archiviazione esterna che vengono collegati ai computer della scuola.

Linee Guida di Buona Condotta/Buone pratiche nell'uso della Rete

- Accesso consentito al Personale Scolastico ad esclusivo uso didattico o di formazione;
 - Accesso consentito agli alunni, sotto la Responsabilità di un Docente;
 - Responsabilità civile e penale dell'utente per l'uso fatto del servizio Internet, a norma delle vigenti Leggi
 - Divieto di installare e/o scaricare sui device software non autorizzati o senza licenza (consultare Animatore Digitale o Responsabile di Laboratorio)
 - Tutela della propria Privacy, quella degli altri utenti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui hai accesso;
 - Rispetto della netiquette (regole condivise che disciplinano il rapportarsi fra utenti della rete, siti, forum, mail e di qualsiasi altro tipo di comunicazione);
 - Controllo della validità e dell'origine delle informazioni a cui si accede o che si ricevono;
 - Utilizzo di fonti alternative di informazione per proposte comparate; ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale e di altri possibili link al sito;
 - Rispetto dei diritti di autore e dei diritti di proprietà intellettuale.
-

3.3 - Strumenti di comunicazione online

Le tecnologie digitali sono in grado di ridefinire gli ambienti di apprendimento, supportando la comunicazione a scuola e facilitando un approccio sempre più collaborativo. L'uso degli strumenti di comunicazione online a scuola, al fianco di quelli più tradizionali, ha l'obiettivo di rendere lo scambio comunicativo maggiormente interattivo e orizzontale. Tale uso segue obiettivi e regole precise correlati alle caratteristiche, funzionalità e potenzialità delle tecnologie digitali.

GESTIONI ACCESSI (PASSWORD, BACKUP. Ecc.)

Sito WEB dell'I.C.2 Vicenza

Il Dirigente Scolastico e il Personale incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato e appropriato.

La Scuola offre all'interno del proprio sito una serie di servizi alle famiglie e ai fruitori esterni.

I Docenti che desiderano pubblicare materiale relativo a buone pratiche, attività didattiche, esperienze particolari, dovranno chiedere l'autorizzazione al Dirigente.

Registro Elettronico dell'I.C.2 Vicenza

I tutori degli alunni della Scuola Secondaria e delle Scuole Primarie hanno accesso al Registro

Elettronico, dove possono trovare e visionare assenze, valutazioni, note ed osservazioni. Inoltre possono trovare lezioni registrate, documenti o approfondimenti. I Genitori sono tenuti a restituire i compiti eseguiti dai propri figli ai Docenti di pertinenza che ne hanno fatto richiesta. Il Registro è uno strumento utilizzato per la comunicazione online individuale o di classe.

Per le famiglie sprovviste di Internet, la Scuola garantisce con puntualità ogni comunicazione.

Piattaforma Gsuite per Alunni dell'I.C.2

Tutti gli alunni della Scuola dell'Infanzia, delle Scuole Primarie e della Scuola Secondaria di I grado utilizzano la piattaforma GSuite, come contenitore di attività/video/materiali didattici (attraverso la *Classroom*) e come mezzo di comunicazione (attraverso l'app *Meet*) con i Docenti

Gli alunni della Secondaria di I grado (previa autorizzazione dei genitori) utilizzano anche le altre applicazioni del pacchetto GSuite, quali *Mail* e *Drive*

L'Istituto supporta, attraverso l'Animatore Digitale ed altre figure preposte, i Genitori che incontrano difficoltà nell'accesso al Registro.

e-mail istituzionale

La posta elettronica istituzionale (fornita ad ogni Docente e al Personale ATA) fornita da GSuite, è strettamente personale, per cui ogni docente dovrà avere cura di uscire dall'account dopo l'utilizzo. E' destinata alla ricezione di comunicazioni, all'invio di documentazione e alla condivisione di materiali, progetti...con altri Docenti o con il Dirigente Scolastico.

Le comunicazioni scuola-famiglia devono avvenire tramite indirizzo istituzionale.

3.4 - Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le studenti/esse e dei docenti (oltre che di tutte le figure professionali che a vario titolo sono inseriti nel mondo della scuola), ed influenzano necessariamente anche la didattica e gli stili di apprendimento. Comprendere il loro utilizzo e le loro potenzialità innovative, diventa di cruciale importanza, anche considerando il quadro di indirizzo normativo esistente e le azioni programmatiche, fra queste il Progetto Generazioni Connesse e il più ampio PNSD.

La presente **ePolicy** contiene indicazioni, revisioni o eventuali integrazioni di Regolamenti già esistenti che disciplinano l'uso dei dispositivi personali in classe, a seconda dei vari usi, anche in considerazione dei dieci punti del Miur per l'uso dei dispositivi mobili a scuola (BYOD, "Bring your own device").

Risulta fondamentale per la comunità scolastica aprire un dialogo su questa tematica e riflettere sulle possibilità per l'Istituto di dotarsi di una regolamentazione condivisa e specifica che tratti tali aspetti, considerando aspetti positivi ed eventuali criticità nella e per la didattica.

Con il DM n. 104 del 30/11/2007 *"Linee di indirizzo e chiarimenti sulla normativa vigente sull'uso di telefoni cellulari e di altri dispositivi elettronici nelle comunità scolastiche"* si chiariva, anche in virtù della normativa allora vigente posta a tutela della privacy, il divieto di utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche allo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali.

E proprio riguardo al Codice della Privacy, Dlgs. 196/2003, modificato e integrato dal D. Lgs. 101/2018 recependo il regolamento UE 2016/679 e art.10 del Codice Civile, è necessario considerare che *"l'uso di cellulari e smartphone è in genere consentito per fini strettamente personali, ad esempio per registrare le lezioni, e sempre nel rispetto delle persone. Spetta comunque agli istituti scolastici decidere nella loro autonomia come regolamentare o se vietare del tutto l'uso dei cellulari. Non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. È bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati. Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line"*.

A rinforzare quanto detto, il ricorso a politiche attive per il BYOD (Bring Your Own Device - "porta il tuo dispositivo") in ambito educativo viene espressamente previsto, attraverso una specifica azione, dal Piano Nazionale Scuola Digitale (PNSD) con l'obiettivo di promuovere una didattica digitale basata sull'integrazione dei dispositivi elettronici personali degli studenti e degli insegnanti (smartphone, tablet e PC portatili) con le dotazioni tecnologiche degli spazi scolastici.

Per gli studenti: Durante le lezioni non è consentito alcun uso di strumenti elettronici personali.

L'utilizzo di device è consentito unicamente a scopo didattico, ad integrazione degli strumenti scolastici disponibili, su richiesta e autorizzazione del docente.

Per i docenti: Durante le lezioni l'utilizzo di device è consentito unicamente a scopo didattico, ad integrazione degli strumenti scolastici disponibili.

Il nostro piano d'azioni

AZIONI (effettuate nell'arco dell'anno scolastico 2021/2022).

Sono state organizzati incontri volti a formare il personale scolastico sul tema delle tecnologie digitali e della protezione dei

- **dati personali**

AZIONI (da sviluppare nell'arco dei tre anni scolastici

successivi). Scegliere almeno 1 di queste azioni:

- **Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse**
Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti
Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte del personale Tecnico Amministrativo e dagli ATA
- **Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali**
- **Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)**
- **Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)**
-
-

Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

4.1 - Sensibilizzazione e Prevenzione

Il rischio online si configura come la possibilità per il minore di:

- commettere azioni online che possano danneggiare se stessi o altri;
- essere una vittima di queste azioni;
- osservare altri commettere queste azioni.

È importante riconoscere questi fenomeni e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per arginarli e contenerli, ma è altrettanto importante sapere quali sono le possibili strategie da mettere in campo per ridurre la possibilità che questi fenomeni avvengano. Ciò è possibile lavorando su aspetti di ampio raggio che possano permettere una riduzione dei fattori di rischio e di conseguenza una minore probabilità che i ragazzi si trovino in situazioni non piacevoli. È importante che abbiano gli strumenti idonei per riconoscere possibili situazioni di rischio e segnalarle ad un adulto di riferimento.

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione**.

- Nel caso della **sensibilizzazione** si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.
- Nel caso della **prevenzione** si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.

Per sensibilizzare le famiglie, l'I.C.2 attiverà iniziative all'uso consapevole delle TIC e della rete, promuovendo la conoscenza delle numerose situazioni di rischio online. A tal fine sono previsti incontri fra docenti e genitori per la diffusione del materiale informativo sulle tematiche trattate. Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di cellulari e smartphone o delle chat line o social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo.

Sul sito icvicenza2.edu.it e sulla pagina relativa a Bullismo/Cyberbullismo e al link "Generazioni connesse" sono condivisi materiali/video dedicati ad alunni, docenti e famiglie che possono fornire

spunti di approfondimento e confronto. La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (Policy e-safety) per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'Istituto e prevenire i rischi legati a un utilizzo non corretto di Internet.

Si prevede di sistemare in ogni plesso dell'Istituto dei BOX in cui gli alunni possano segnalare eventuali disagi/preoccupazioni/presunti casi di cyberbullismo.

Azioni di prevenzione

- installazione di filtri sul server e sul motore di Ricerca
- blocco di finestre pop up
- verifica della cronologia
- utilizzo di cloud

Azioni di sensibilizzazione

Educare la comunità scolastica a:

- un uso consapevole e responsabile della rete
- proteggere la propria identità,
- creare password efficaci,
- riflettere sulle possibili conseguenze prima di postare foto o video propri e non postare foto e video di altri senza il loro consenso,
- rispettare il copyright, e citare le fonti,
- insegnare a riconoscere e a confidarsi con adulti di riferimento rispetto a situazioni di rischio,
- conoscere i servizi messi a disposizione dal Safer Internet Center per segnalazioni, anche anonime, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la rete,
- "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children e della linea di ascolto 1.96.96 di Telefono Azzurro legati all'uso delle nuove tecnologie digitali e alla sicurezza online.

I docenti si impegnano

- ad accompagnare gli alunni nella navigazione in Rete;
- creare degli spazi in cui gli alunni si possono confrontare sulle tematiche del cyberbullismo, utilizzando come spunti video/canzoni..;
- confrontarsi tra docenti della classe e/o con esperti del territorio.

link del sito <https://icvicenza2.edu.it/bullismo-cyberbullismo/> in cui sono presenti:

- moduli segnalazione
- indirizzo mail per segnalazioni;
- Linee di Orientamento per Azioni di contrasto al Bullismo/Cyberbullismo
- Linee Guida per l'uso positivo delle tecnologie digitali e la prevenzione dei rischi nelle scuole
- proposte attività

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

La stessa legge e le relative **Linee di orientamento per la prevenzione e il contrasto del cyberbullismo** indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo. Le linee prevedono:

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di [cyberbullismo](#) e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
 - Ha il compito di coordinare le iniziative di prevenzione e contrasto del [cyberbullismo](#). A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
 - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

All'I.C.2 Vicenza è presente un team per il contrasto al bullismo e cyberbullismo che monitora la situazione ed invita i docenti a svolgere delle attività nelle classi per la prevenzione di tale fenomeno.

L'I.C.2 Vicenza, all'interno del Progetto *Scuola Amica dei Bambini e delle Bambine*, ha svolto e svolge attività di prevenzione al cyberbullismo e bullismo partendo dalla conoscenza di questo fenomeno: le proposte educative hanno coinvolto tutti gli alunni, dall'Infanzia alla Secondaria, in modi diversi ed adeguati alle età.

4.3 - Hate speech: che cos'è e come prevenirlo

Il fenomeno di “incitamento all’odio” o “discorso d’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 appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine “hate speech” indica un’offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l’obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all’orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l’impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

Questi i punti salienti del documento [No hate Ita](#) (tratto da www.generazioneconnesse.it, “Bookmarks. A manual for combating hate speech on line through human rights education”, edito dal Consiglio d’Europa) che spiegano il fenomeno:

- **Il discorso d’odio procura sofferenza.** La parola ferisce, e a maggior ragione l’odio!
- **Gli atteggiamenti alimentano gli atti.** Il discorso dell’odio è pericoloso anche perché può condurre a più gravi violazioni dei diritti umani, e perfino alla violenza fisica.

- **L'odio online non è solo espresso a parole.** Internet ci permette di comunicare rapidamente e in modi svariati ed in maniera anonima.
- **L'odio prende di mira sia gli individui che i gruppi.** L'odio online può prendere di mira dei gruppi che spesso sono già vulnerabili sotto altri aspetti, ma anche i singoli individui sono sempre maggiormente oggetto di attacchi.
- **Internet è difficilmente controllabile.** La diffusione di messaggi di incitamento all'odio è maggiormente tollerata su Internet rispetto al mondo offline ed è sottoposta a minori controlli.
- **Ha radici profonde.** Gli atteggiamenti e le tensioni sociali che suscitano sentimenti di odio online affondano le loro radici nella società, e non sono diversi, in genere, da quelli che alimentano il discorso dell'odio offline.
- **Impunità e anonimato.** Queste abbassano le remore etiche. In realtà, però, qualsiasi azione compiuta sul web consente di rintracciare il suo autore.

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.

Facendo riferimento a quanto proposto da "Generazione Connesse" e al materiale presente nella piattaforma Elisa, per il percorso di formazione per referenti per il contrasto del Bullismo e Cyberbullismo organizzato dal MIUR e dall'Università di Firenze-Dipartimento di Formazione, Lingue, Intercultura, Letteratura e Psicologia, vengono proposti ai docenti e quindi agli studenti percorsi di riflessione e confronto su questa tematica.

Occorre in tal senso fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, e promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo 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.

La S.I.I.Pa.C., la [Società Italiana Intervento Patologie Compulsive](http://www.generazioneconnesse.it), (tratto da www.generazioneconnesse.it) definisce la dipendenza da Internet come progressivo e totale assorbimento del soggetto alla Rete; di seguito alcune caratteristiche specifiche:

- **Dominanza.** L'attività domina i pensieri ed il comportamento del soggetto, assumendo un valore primario tra tutti gli interessi.
- **Alterazioni del tono dell'umore.** L'inizio dell'attività provoca cambiamenti nel tono dell'umore. Il soggetto prova un aumento d'eccitazione o maggiore rilassatezza come diretta conseguenza dell'incontro con l'oggetto della dipendenza.
- **Conflitto.** Conflitti inter-personali tra il soggetto e coloro che gli sono vicini, conflitti intra-personali interni a se stesso, a causa del comportamento dipendente.
- **Ricaduta.** Tendenza a ricominciare l'attività dopo averla interrotta.

Oltre ad interventi specifici con esperti esterni, all'interno delle normali attività curricolari, sono state previste **azioni** di informazione in merito a quella che può diventare una vera e propria patologia che compromette la salute e le relazioni sociali.

4.5 - Sexting

Il "sexting" è fra i rischi più diffusi connessi ad un uso poco consapevole della Rete. Il termine indica un fenomeno molto frequente fra i giovanissimi che consiste nello scambio di contenuti medialmente sessualmente espliciti; i/le ragazzi/e lo fanno senza essere realmente consapevoli di scambiare materiale (pedopornografico) che potrebbe arrivare in mani sbagliate e avere conseguenze impattanti emotivamente per i protagonisti delle immagini, delle foto e dei video.

Il sexting (abbreviazione di sex – sesso e texting – messaggiare, inviare messaggi) indica l'invio e/o la ricezione di contenuti (video o immagini) sessualmente espliciti che ritraggono se stessi o gli altri.

"Spesso sono realizzate con il telefonino, e vengono diffuse attraverso il cellulare (tramite invio di mms o condivisione tramite bluetooth) o attraverso siti, e-mail, chat. Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile e possono creare seri problemi, sia personali che legali, alla persona ritratta. L'invio di foto che ritraggono

minorenni al di sotto dei 18 anni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico”.

Facendo riferimento a quanto proposto da "Generazione Connesse" e al materiale presente nella piattaforma Elisa, per il percorso di formazione per referenti per il contrasto del Bullismo e Cyberbullismo organizzato dal MIUR e dall'Università di Firenze - Dipartimento di Formazione, Lingue, Intercultura, Letteratura e Psicologia, vengono proposti ai docenti, e quindi agli studenti, percorsi di riflessione e confronto su questa tematica.

Azioni

- verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione;
 - sensibilizzazione sulla necessità di monitorare la presenza sui social dei figli.
 - verso gli alunni: inserimento nel curriculum di temi legati all'affettività, alla sessualità e alle differenze di genere, secondo le età degli alunni.
-

4.6 - Adescamento online

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenzialmente abusanti utilizzano 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 spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di ***teen dating*** (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

In Italia l'adescamento si configura come reato dal 2012 (art. 609-undecies – l'adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell'adescamento.

Il miglior modo per prevenire casi di adescamento online è accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. Ciò aiuterebbe a renderli più

sicuri emotivamente e pronti ad affrontare eventuali situazioni a rischio, imparando innanzitutto a gestire le proprie emozioni, il rapporto con il proprio corpo e con gli altri. È molto importante, inoltre, che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e della sessualità.

L'I.C. 2 propone ogni anno un Percorso di *Affettività e Sessualità* per gli alunni delle classi Quinte della Scuole Primarie e per gli alunni delle classi Terze della Scuola Secondaria di I grado, gestito da un esperto, individuato attraverso apposito Bando.

Azioni:

- sensibilizzazione sull'esistenza di individui che usano la Rete per instaurare relazioni, virtuali o reali, non corrette con i minori;
- messa a disposizione degli alunni BOX per eventuali preoccupazioni/segnalazioni/dubbi in merito.

4.7 - Pedopornografia

La pedopornografia online è un reato (art. 600-ter comma 3 del c.p.) che consiste nel produrre, divulgare, diffondere e pubblicizzare, anche per via telematica, immagini o video ritraenti bambini/e, ragazzi/e coinvolti/e in comportamenti sessualmente espliciti, **concrete o simulate** o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

La legge n. 269 del 3 agosto 1998 *“Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di schiavitù”,* introduce nuove fattispecie di reato (come ad esempio il turismo sessuale) e, insieme alle successive modifiche e integrazioni contenute nella **legge n. 38 del 6 febbraio 2006** *“Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet”,* segna una tappa fondamentale nella definizione e predisposizione di strumenti utili a contrastare i fenomeni di sfruttamento sessuale a danno di minori. Quest'ultima, introduce, tra le altre cose, il reato di “pornografia minorile virtuale” (artt. 600 ter e 600 quater c.p.) che si verifica quando il materiale pedopornografico rappresenta immagini relative a bambini/e ed adolescenti, realizzate con tecniche di elaborazione grafica non associate, in tutto o in parte, a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.

Secondo la Legge 172/2012 - Ratifica della Convenzione di Lanzarote (Art 4.) per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali.

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere.

La pedopornografia è tuttavia un fenomeno di cui si deve sapere di più, ed è utile parlarne, in particolare se si vogliono chiarire alcuni aspetti legati alle conseguenze impreviste del sexting.

Inoltre, è auspicabile che possa rientrare nei temi di un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico promuovendo i servizi di Generazioni Connesse: qualora navigando in Rete si incontri materiale pedopornografico è opportuno segnalarlo, anche anonimamente, attraverso il sito www.generazioniconnesse.it alla sezione **"Segnala contenuti illegali"** ([Hotline](#)).

Il servizio Hotline si occupa di raccogliere e dare corso a segnalazioni, inoltrate anche in forma anonima, relative a contenuti pedopornografici e altri contenuti illegali/dannosi diffusi attraverso la Rete. I due servizi messi a disposizione dal Safer Internet Centre sono il "Clicca e Segnala" di [Telefono Azzurro](#) e "STOP-IT" di [Save the Children](#).

In un'ottica di attività preventive, il tema della pedopornografia è estremamente delicato, occorre parlarne sempre in considerazione della maturità, della fascia d'età e selezionando il tipo di informazioni che si possono condividere. Ad esempio, non è utile diffondere tra i bambini e le bambine più piccoli/e l'uso di servizi come le hotline, sia perché in caso di visione accidentale di materiale pedopornografico è opportuno che bambini/e e ragazzi/e possano parlarne con gli adulti di riferimento per la migliore risposta possibile, sia perché si potrebbe incentivare la ricerca proattiva, che comunque è vietata dalla legge italiana, per minori e per adulti.

Risulta utilissima l'attività educativa sull'affettività e le relazioni, sottolineando sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio.

Facendo riferimento a quanto proposto da "Generazione Connesse" e al materiale presente nella piattaforma *Elisa*, per il percorso di formazione per referenti per il contrasto del Bullismo e Cyberbullismo organizzato dal MIUR e dall'Università di Firenze - Dipartimento di Formazione, Lingue, Intercultura, Letteratura e Psicologia, vengono proposti ai docenti e quindi agli studenti percorsi di riflessione e confronto su questa tematica.

Azioni

verso i genitori:

- informazione circa le possibilità di attivare forme di controllo parentale della navigazione;
- sensibilizzazione sulla necessità di monitorare la presenza sui social dei figli.

verso gli alunni:

- inserimento nel curriculum di temi legati all'affidabilità delle fonti online e alla sessualità.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2022/2023).

Scegliere almeno 1 di queste azioni:

- ☐ **Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.**
- ☐ **Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/le studenti/studentesse, con il coinvolgimento di esperti.**
- ☐ **Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.**
- ☐ **Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.**
- ☐ **Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse.**

AZIONI (da sviluppare nell'arco dei tre anni scolastici

successivi). Scegliere almeno 1 di queste azioni:

- ☐ **Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/le studenti/studentesse, con il coinvolgimento di esperti.**
- ☐ **Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.**
- ☐ **Promuovere incontri e laboratori per studenti e studentesse dedicati all'Educazione Civica Digitale.**
- ☐ **Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/le studenti/studentesse**

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

Questa sezione dell'ePolicy contiene le procedure standardizzate per la segnalazione e gestione dei problemi connessi a comportamenti online a rischio di studenti e studentesse (vedi allegati a seguire).

Tali procedure dovranno essere una guida costante per il personale della scuola nell'identificazione di una situazione online a rischio, così da definire le modalità di presa in carico da parte della scuola e l'intervento migliore da mettere in atto per aiutare studenti/esse in difficoltà. Esse, inoltre, forniscono valide indicazioni anche per i professionisti e le organizzazioni esterne che operano con la scuola (vedi paragrafo 1.3. dell'ePolicy).

Nelle procedure:

- sono indicate le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso.**
- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola **individua le figure che costituiranno un team** preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Tali procedure sono comunicate e condivise con l'intera comunità scolastica.

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

La condivisione avverrà attraverso assemblee scolastiche che coinvolgono i genitori, gli studenti e le studentesse e il personale della scuola, con l'utilizzo di locandine da affiggere a scuola, attraverso news nel sito della scuola e durante i collegi docenti e attraverso tutti i canali maggiormente utili ad un'efficace comunicazione.

A seguire, le problematiche a cui fanno riferimento le procedure allegate:

- **Cyberbullismo:** è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online:** se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting:** nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore ultraquattordicenne (o i suoi genitori o chi esercita la responsabilità del minore) che sia stato vittima di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti diffusi nella Rete. Se entro 24 ore il gestore non avrà provveduto, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore.

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di [Helpline 19696](#) e [Chat di Telefono Azzurro](#) per supporto ed emergenze;
- [Clicca e segnala di Telefono Azzurro](#) e [STOP-IT di Save the Children Italia](#) per segnalare la presenza di materiale pedopornografico online.

Presso l'I.C. 2 Vicenza sono state individuate le docenti Fontana Laura e Garbin Federica quali referenti del Team dedicato alla Prevenzione al Bullismo/Cyberbullismo, preposte alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti).

Le Referenti coordinano e promuovono iniziative specifiche per la prevenzione ed il contrasto del bullismo e del cyberbullismo e coinvolgono studenti, colleghi e genitori in progetti e percorsi formativi.

La rilevazione dei casi è compito di ciascuno, qualora fosse testimone di situazioni da segnalare.

Il Personale Docente e ATA deve essere figura accogliente cui poter fare riferimento: è auspicabile pertanto evitare atteggiamenti accusatori per riuscire a ricevere dai minori più fragili eventuali segnalazioni. Inoltre gli adulti sono chiamati a vigilare su problematiche/rischi, che gli alunni possono vivere e affrontare ogni giorno.

Accorgersi tempestivamente di quanto accade ed intervenire prontamente con **azioni** di contrasto verso gli atti inopportuni/illegali, diventa fondamentale per poter evitare conseguenze a lungo termine che possano compromettere il benessere dei bambini/ragazzi coinvolti.

5.2. - Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non è circoscritto all'ambito dell'apprendimento, ossia alla sola preparazione e tenuta delle lezioni, alla verifica/valutazione dei contenuti appresi dagli studenti e dalle studentesse, ma si estende a tutte le altre attività educative.

Le situazioni problematiche in relazione all'uso delle tecnologie digitali dovrebbero essere sempre gestite anche a livello di gruppo.

Come descritto nelle procedure di questa sezione, si potrebbero palesare due casi:

- CASO A (SOSPETTO) – Il docente ha il sospetto che stia avvenendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.
- CASO B (EVIDENZA) – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

Per tutti i dettagli fate riferimento agli allegati con le procedure.

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola può prevedere alcuni strumenti di segnalazione ad hoc messi a loro disposizione:

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito [1.96.96](tel:19696).

Nel sito della Scuola sono presenti i moduli per la segnalazione di eventuali casi di bullismo/cyberbullismo.

La Comunità Scolastica è annualmente messa al corrente, attraverso apposita circolare, della presenza di tali modelli.

L'indirizzo mail per l'invio è il seguente: icvicenza2.bullismo.cyber@gmail.com

Nella circolare vengono anche indicate le figure referenti.

In box dedicati all'interno della Scuola è possibile inserire le segnalazioni che anche gli alunni possono indicare, compilando i moduli presenti nelle vicinanze.

5.3. - Gli attori sul territorio

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il [Vademecum](#) di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

- **Comitato Regionale Unicef:** laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni):** svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale:** supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni:** accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali:** forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico:** segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni:** segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

Associazioni/Enti sul Territorio

www.generazioneconnesse.it

www.commissariatops.it

5.4. - Allegati con le procedure

Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



Procedure interne: cosa fare in caso di evidenza di Cyberbullismo



Il docente ha evidenza che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Avvisa il referente per il cyberbullismo (e/o il referente indicato nell'ePolicy) e il Dirigente Scolastico che convoca il CDC.

A) Se c'è fattispecie di reato - seguite le procedure della scuola

B) Se non c'è fattispecie di reato

- Richiedi la consulenza dello psicologo/a scolastico

- Informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo/a, su quanto accade e condividetevi informazioni e strategie.

- Informa i genitori di ragazzi/e infra quattordicenni della possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy)

- Attiva il consiglio di classe.

- Valuta come coinvolgere gli operatori scolastici su quanto sta accadendo.

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

NELLE CLASSI

- Cerca di capire il livello di diffusione dell'episodio nell'Istituto e parla della necessità di non diffondere ulteriormente online i materiali.

- Parla del cyberbullismo e delle sue conseguenze (non nominare gli alunni coinvolti). Suggestisci di chiedere aiuto per situazioni di questo tipo. Prevedi un momento laboratoriale in modo da facilitare l'elaborazione della situazione.

- a seconda della situazione trova il modo di supportare la vittima e di responsabilizzare i compagni rispetto al loro ruolo, anche di spettatori, nella situazione.



A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, segnala alla Polizia Postale:

a) contenuto; b) modalità di diffusione.

Se è opportuno, richiedi un sostegno ai servizi territoriali o ad altre Autorità competenti (soprattutto se il cyberbullismo non si limita alla scuola).

© All rights reserved Generazioni Connesse 2019



Procedure interne: cosa fare in caso di sospetto di Cyberbullismo



Il docente sospetta che stia accadendo qualcosa tra gli studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo

Sonda il clima di classe, ascoltando i ragazzi e monitorando ciò che accade (ma senza fare indagini o interrogatori).

Cerca di capire il livello di diffusione dell'episodio a livello di Istituto.

Condividi con il referente per il cyberbullismo (e/o il referente indicato nell'e-policy): valuta con lui/loro le possibili strategie di intervento.

Valuta se è il caso di avvisare il consiglio di classe.

Valuta se è il caso di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate.

Se, come docente, hai un dubbio su come procedere o interpretare quello che sta accadendo, puoi chiedere in qualsiasi momento, una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Parla in classe del cyberbullismo e delle sue conseguenze (non nominare gli alunni che sospetti coinvolti). Suggestisci di **chiedere aiuto** per situazioni di questo tipo. Proponi attività in classe sull'empatia e sul riconoscimento delle emozioni (proprie e altrui)

Se emergono evidenze passa allo schema successivo

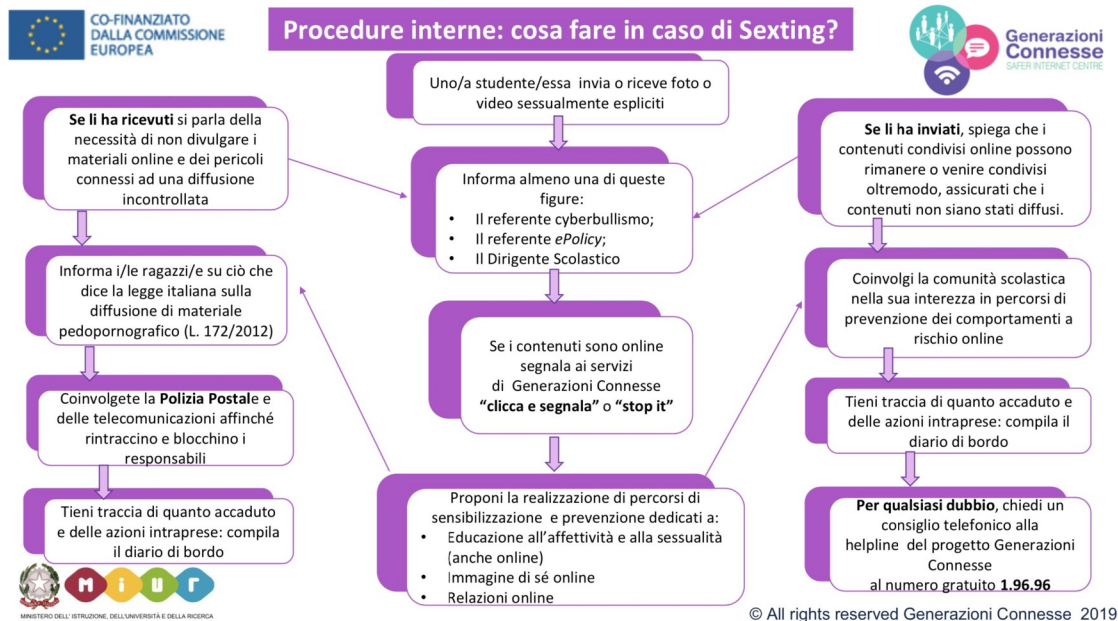
Informa i/le ragazzi/e su ciò che dice la legge italiana su cyberbullismo L. 71/2017
Ricorda agli studenti che possono segnalare al gestore del sito/social e al garante privacy eventuali contenuti offensivi/lesivi che li riguardano

Ricorda a studenti/esse che possono chiedere in qualsiasi momento una consulenza telefonica alla helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96 o via chat

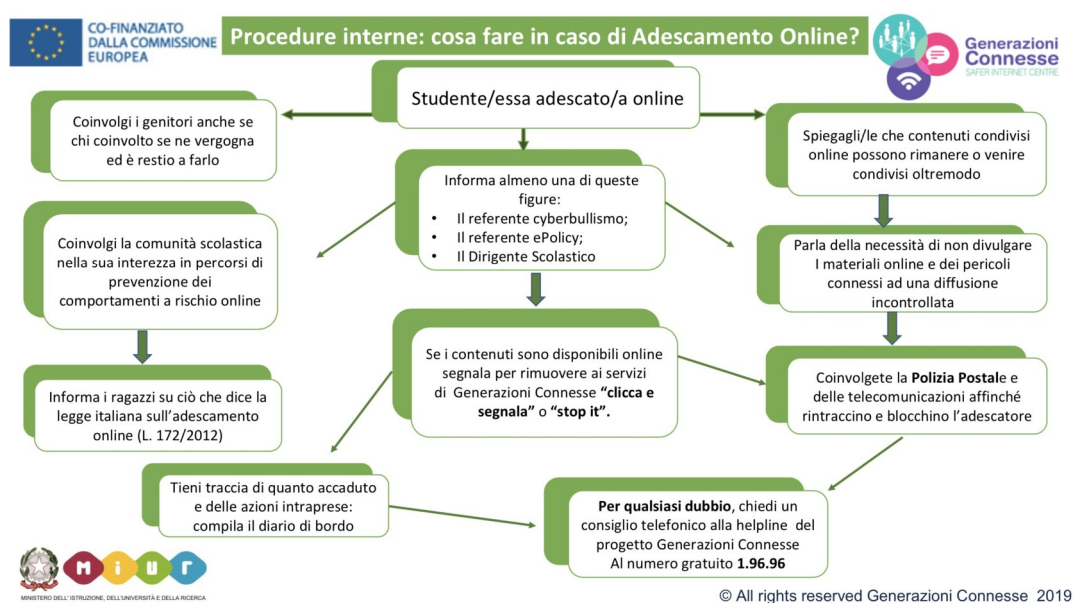


© All rights reserved Generazioni Connesse 2019

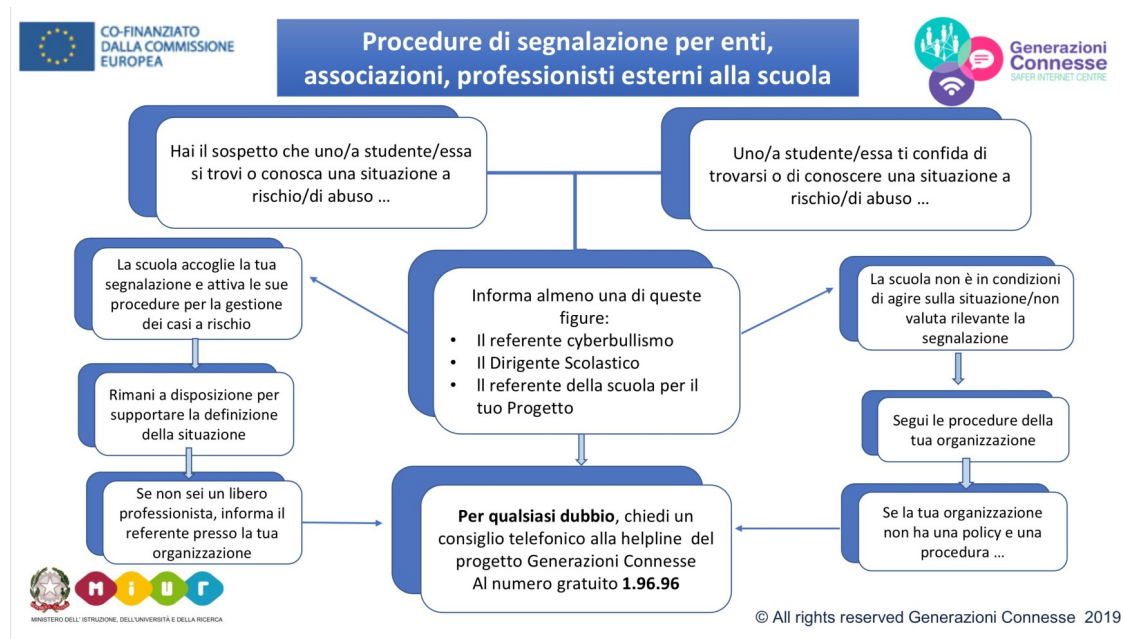
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Altri allegati

- [Scheda di segnalazione](#)
- [Diario di bordo](#)
- [iGloss@ 1.0 l'ABC dei comportamenti devianti online](#)
- [Elenco reati procedibili d'ufficio](#)

Sul sito e ai link di seguito elencati, sono presenti

Modelli per le segnalazioni di presunti casi di bullismo/cyberbullismo

- **per alunni:**

<https://icvicenza2.edu.it/wp-content/uploads/sites/131/segnalazione-atti-di-bullismo-alun-.docx>

- **per genitori/insegnanti:**

<https://icvicenza2.edu.it/wp-content/uploads/sites/131/segnalazione-atti-di-bullismo-genitori-insegnanti.docx>

Modello per la valutazione approfondita da parte del **Team** per la Prevenzione al Bullismo/Cyberbullismo

<https://icvicenza2.edu.it/wp-content/uploads/sites/131/scheda-di-valutazione-approfondita.pdf>

Scheda Monitoraggio

<https://icvicenza2.edu.it/wp-content/uploads/sites/131/scheda-di-monitoraggio-I.C.2.pdf>

Procedura per caso di bullismo/cyberbullismo e fenomeni legati all'uso improprio della Rete

<https://icvicenza2.edu.it/wp-content/uploads/sites/131/intervento-quali-quali.pdf>

Classificazione del caso

<https://icvicenza2.edu.it/wp-content/uploads/sites/131/valutazione-della-gravità.pdf>

Scelta dell'intervento

<https://icvicenza2.edu.it/wp-content/uploads/sites/131/scelta-intervento-sulla-base-della-gravità.pdf>

Figure preposte agli interventi

<https://icvicenza2.edu.it/wp-content/uploads/sites/131/attori-coinvolti-nellintervento.pdf>

Supporto Intensivo a Lungo Termine

<https://icvicenza2.edu.it/wp-content/uploads/sites/131/supporto-intensivo-a-lungo-termini-e-di-rete.pdf>

Modello per il Monitoraggio

Il nostro piano d'azioni

Creare in periodi stabiliti Monitoraggi sullo Star Bene a Scuola

Firmato digitalmente da ALFONSO SFORZA