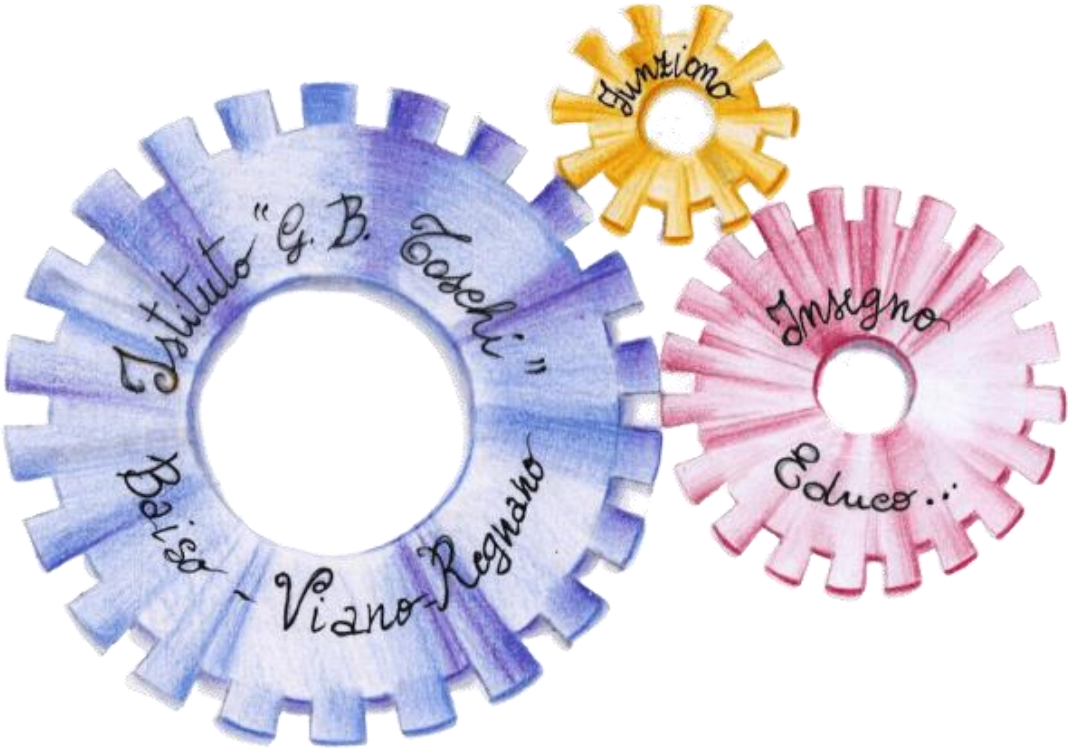
ISTITUTO COMPRENSIVO "G.B. TOSCHI" BAISO - VIANO
Dirigenza e segreteria: Via Ca' Toschi 4 - 42031 Baiso (RE)
C.F. 80015710355 – tel. 0522/993571-993572 – Sito Web: www.ictoschi.edu.it
Mail: reic819003@istruzione.it – reic819003@pec.istruzione.it

E-Safety Policy



Misure atte a facilitare e promuovere l'utilizzo positivo delle TIC nella didattica e negli ambienti scolastici.

Misure di prevenzione e misure di gestione di situazioni problematiche relative all'uso delle tecnologie digitali.

INDICE

E-Safety Policy

1. Introduzione

1.1. Scopo della Policy;
1.2. Ruoli e Responsabilità;
1.3. Condivisione e comunicazione della Policy all'intera comunità scolastica;
1.4. Gestione delle infrazioni alla Policy;
1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento;
1.6. Integrazione della Policy con Regolamenti esistenti.

2. Formazione e Curricolo

2.1. Curricolo sulle competenze digitali per gli studenti;
2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali;
2.3. Sensibilizzazione delle famiglie.

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

3.1. Protezione dei dati personali;
3.2. Accesso ad Internet;
3.3. E-mail;
3.4. Blog e sito web della scuola;
3.5. Social network;
3.6. Utilizzo di supporti magnetici;
3.7. Utilizzo delle stampanti e dei materiali d'uso;
3.8. BYOD Regolamento per l'utilizzo dei dispositivi digitali personali a scuola;
3.9. Strumenti di comunicazione online.

4. Strumentazione personale

4.1. Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc...;
4.2. Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc...;
4.3. Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.

5. Prevenzione, rilevazione e gestione dei casi

5.1. Rischi;
5.2. Azioni;
5.3. Che cosa segnalare;
5.4. Come segnalare: quali strumenti e a chi;
5.5. Gestione dei casi;
5.6. Gli attori sul territorio;
5.7. Allegati e procedure.

1. Introduzione

La scuola elabora il presente documento seguendo le indicazioni delle Linee di Orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo (aprile 2015) elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con "Generazioni Connesse" e il Safer Internet Center per l'Italia. Si recepiscono, altresì, le integrazioni e le modifiche necessarie in linea con i recenti interventi normativi con particolare riferimento alle innovazioni introdotte con l'emanazione della L. 71/2017 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" e DM 18/2021 “Line di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo”.

Tale documento è da intendersi quale strumento flessibile e suscettibile di periodici aggiornamenti tale da rispondere alle sfide educative e pedagogiche derivanti dall'evolversi costante e veloce delle nuove tecnologie.

1.1. Scopo della Policy

La Policy ha lo scopo di educare e sensibilizzare tutti gli attori in campo, dagli adolescenti, a tutto il personale scolastico, fino ai genitori, all'uso sicuro e consapevole di Internet.

Le giovani generazioni di "nativi digitali" imparano a familiarizzare con le tecnologie fin dall'infanzia, spesso inconsapevoli dei rischi presenti nella rete. Gli insegnanti, che grazie all'uso delle TIC hanno l'opportunità di promuovere l'inclusione e l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione, hanno anche la responsabilità di guidare gli studenti nelle attività online e di stabilire obiettivi chiari per un uso responsabile di Internet.

Il documento si pone pertanto come finalità la promozione di un uso consapevole e critico delle tecnologie digitali e di Internet, l'acquisizione di procedure e competenze tecniche, nonché corrette norme comportamentali, senza trascurare la prevenzione, la rilevazione e la gestione di situazioni problematiche relative all'uso di tali tecnologie.

Nello specifico, la nostra Policy di e-Safety avrà lo scopo di delineare:

1. **misure atte a facilitare e promuovere** l'utilizzo delle TIC nella didattica, cioè azioni utili a sviluppare le competenze digitali, che costituiscono anche misure di prevenzione, come si vedrà più avanti;
2. **misure di prevenzione**, ossia azioni finalizzate alla prevenzione nella scuola di fenomeni legati ai rischi delle tecnologie digitali (che includano iniziative volte a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, dell'utilizzo positivo e responsabile

delle Tecnologie dell'Informazione e della Comunicazione (TIC), ecc…);

3. **misure per la segnalazione dei casi**, ovvero disposizioni semplici su come segnalare i casi nella scuola, comprese informazioni su chi sono le figure di riferimento, sugli strumenti a disposizione, sull'iter successivo alla segnalazione e su quali misure di tutela può contare chi segnala;
4. **misure per la gestione dei casi**, ossia le misure che la scuola attiva a supporto di chi subisce e chi attua azioni, delle famiglie e di tutti coloro che sono stati spettatori attivi o passivi di quanto avvenuto; misure che disciplinano anche il coinvolgimento di attori esterni quali le forze dell'ordine e i servizi sociali.

Questa Policy si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici della scuola.

L'Istituto opera in stretto collegamento con le forze dell'ordine, con la Procura della Repubblica, con istituzioni del settore educativo, per mettere in campo strategie di prevenzione al bullismo e cyberbullismo e interventi di recupero nel caso in cui vengano individuati tali fenomeni, informando i genitori/tutori e chiedendo la loro collaborazione anche qualora gli episodi si siano verificati al di fuori delle attività didattiche.

1.2. Ruoli e responsabilità

Dirigente Scolastico

Il ruolo del Dirigente Scolastico nel promuovere l'uso delle tecnologie e di Internet include i seguenti compiti:

- ✓ garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- ✓ garantire che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente l'insegnamento volto a promuovere una cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, nonché un utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della comunicazione (TIC);
- ✓ garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- ✓ comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

Referente per le attività di prevenzione e contrasto al bullismo e cyberbullismo (MIUR AOODGSIP. Registro Ufficiale prot. 964 del 24.2.2017) e Animatore digitale

Il ruolo del Referente per le attività di prevenzione e contrasto al bullismo e cyberbullismo, in collaborazione con l'Animatore digitale, include i seguenti compiti:

- ✓ fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- ✓ monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di Internet a scuola;
- ✓ assicurare che gli utenti possano accedere alla rete della scuola solo tramite password applicate e regolarmente cambiate;
- ✓ curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione).

Docenti

Il ruolo del personale docente, fermo restando la libertà d'insegnamento, include i seguenti compiti:

- ✓ informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- ✓ garantire che gli alunni comprendano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di Internet;
- ✓ garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;
- ✓ assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- ✓ controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- ✓ nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- ✓ far nascere nella componente studentesca una buona cognizione della proprietà del software e delle normative sul diritto d'autore nonché far comprendere la necessità di effettuare ricerche sul web e la relativa estrazione di documenti evitando il plagio o l'illecita diffusione di dati

personali;

- ✓ comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- ✓ non divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete Wi-Fi;
- ✓ non allontanarsi dalla postazione lasciandola incustodita, se non prima di aver effettuato la disconnessione;
- ✓ non salvare sulla memoria locale (hard disk interni o supporti di memoria esterni come USB) delle postazioni file contenenti dati personali e/o sensibili;
- ✓ non fare uso di dispositivi di carattere personale (telefoni cellulari/tablet) in servizio se non per esclusivo uso didattico;
- ✓ segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo al Referente d'istituto per il bullismo e il cyberbullismo ai fini della ricerca di buone pratiche e soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- ✓ segnalare al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di Internet, per l'adozione delle procedure previste dalle norme.

Alunni

Il ruolo degli alunni include i seguenti compiti:

- ✓ essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- ✓ comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi;
- ✓ adottare condotte rispettose degli altri anche quando si comunica in rete;
- ✓ non eseguire tentativi di modifica della configurazione di sistema delle macchine;
- ✓ non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
- ✓ non utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante;

- ✓ esprimere domande o difficoltà o richieste di aiuto nell'utilizzo delle tecnologie didattiche o di Internet rivolgendosi ai docenti e ai genitori.

Genitori

Il ruolo dei genitori degli alunni include i seguenti compiti:

- ✓ sostenere la linea di condotta adottata dalla scuola nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- ✓ seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllando l'utilizzo del pc e di Internet;
- ✓ concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di Internet;
- ✓ fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di Internet e del telefono cellulare in generale.

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

L'Istituto si impegna a pubblicare sul sito della scuola il presente documento.

Inoltre, si prevede di:

1) Condividere e comunicare la politica di e-safety agli alunni:

- ✓ tutti gli alunni saranno informati che la rete, l'uso di Internet e di ogni dispositivo digitale saranno controllati dagli insegnanti e utilizzati solo con la loro autorizzazione;
- ✓ l'istruzione degli alunni riguardo all'uso responsabile e sicuro di Internet precederà l'accesso alla rete;
- ✓ l'elenco delle regole per la sicurezza on-line sarà pubblicato in tutte le aule o laboratori con accesso a Internet;
- ✓ sarà data particolare attenzione nell'educazione sulla sicurezza agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili.

2) Condividere e comunicare la politica di e-safety al personale:

- ✓ la linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di Internet sarà discussa negli organi collegiali preposti e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web;
- ✓ un'adeguata informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di Internet, sia professionalmente che personalmente, sarà fornita a tutto il

personale, anche attraverso il sito web della scuola;

- ✓ tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

3) Condividere e comunicare la politica di e-safety ai genitori:

- ✓ l'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di Internet sarà richiamata nelle news o in altre aree del sito web della scuola;
- ✓ sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di Internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali;
- ✓ il Referente per le attività di prevenzione e contrasto al bullismo e cyberbullismo fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di Internet anche a casa;
- ✓ i docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero.

1.4. Gestione delle infrazioni alla Policy

Per la componente alunni, le infrazioni verranno sanzionate come da Regolamento di Istituto pubblicato sul sito web della scuola. Il Dirigente Scolastico ha la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (pc, tablet, notebook, ecc…) a chi non si attiene alle regole stabilite.

In genere, l'Istituzione scolastica può adottare provvedimenti, proporzionati all'età e alla gravità del comportamento, quali:

- ✓ il richiamo verbale;
- ✓ il richiamo verbale con conseguenze quali riduzione o sospensione dell'attività gratificante;
- ✓ il richiamo scritto con annotazione sul diario e/o suo Registro Elettronico;
- ✓ la convocazione dei genitori da parte degli insegnanti e/o del Dirigente Scolastico;
- ✓ ritiro del device fino al termine della giornata scolastica;

I genitori sono invitati a supportare la scuola per mettere a punto azioni di contrasto efficaci. Nel caso di infrazioni alla Policy si prevedono interventi, che vanno dalla semplice comunicazione del problema, alla convocazione e colloquio con il docente o il Dirigente Scolastico.

Per quanto riguarda il personale scolastico, le infrazioni alla Policy saranno gestite direttamente dal Dirigente Scolastico.

Qualora le infrazioni alla Policy si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti in competenza. Si ricorda, infatti, che nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361).

I reati che, in ambiente scolastico, possono essere riferiti all'ambito digitale e commessi per via telematica sono tra gli altri:

- ✓ minaccia, in particolare, se la minaccia è grave, per tale reato si procede d'ufficio (art. 612 codice penale);
- ✓ induzione alla prostituzione minorile (art. 600bis);
- ✓ pedopornografia (art. 600ter);
- ✓ corruzione di minorenne (art. 609quinquies).

  Per i reati sessuali la magistratura di norma procede su querela di parte; tuttavia nei casi più gravi si persegue d'ufficio e in genere i reati verso le/i minori sono tra quelli per i quali si procede d'ufficio.

1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il monitoraggio dell'implementazione della Policy sarà compito del Referente per le attività di prevenzione e contrasto del bullismo e cyberbullismo. Si avranno inoltre degli aggiornamenti, laddove necessario e secondo una logica di condivisione e partecipazione attiva, sentito il parere degli insegnanti e viste le esigenze delle famiglie.

1.6. Integrazione della Policy con Regolamenti esistenti

La presente Policy si integra pienamente con il Piano Triennale dell'Offerta Formativa, il Regolamento interno di Istituto e il Patto di Corresponsabilità.

2. Formazione e Curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

L'Istituto persegue, relativamente al curricolo digitale, le recenti indicazioni del PNSD: "*Definire le competenze di cui i nostri studenti hanno bisogno è una sfida ben più ampia e strutturata di quella che il sentire comune sintetizza nell'uso critico della Rete, o nell'informatica. Dobbiamo*

affrontarla partendo da un'idea di competenze allineata al ventunesimo secolo: fatta di nuove alfabetizzazioni, ma anche e soprattutto di competenze trasversali e di attitudini da sviluppare. In particolare, occorre rafforzare le competenze relative alla comprensione e alla produzione di contenuti complessi e articolati anche all'interno dell'universo comunicativo digitale, nel quale a volte prevalgono granularità e frammentazione. Proprio per questo è essenziale lavorare sull'alfabetizzazione informativa e digitale (information literacy e digital literacy), che mettono al centro il ruolo dell'informazione e dei dati nello sviluppo di una società interconnessa basata sulle conoscenze e l'informazione. È in questo contesto che occorre guardare alle sfide rappresentate dal rapporto fra pubblico e privato, dal rapporto tra creatività digitale e artigianato, e tra imprenditorialità digitale, manifattura e lavoro. Ed è ancora in questo contesto che va collocata l'introduzione al pensiero logico e computazionale e la familiarizzazione con gli aspetti operativi delle tecnologie informatiche. In questo paradigma, gli studenti devono essere utenti consapevoli di ambienti e strumenti digitali, ma anche produttori, creatori, progettisti. E i docenti, dalla loro parte e in particolare per quanto riguarda le competenze digitali, dovranno essere messi nelle giuste condizioni per agire come facilitatori di percorsi didattici innovativi basati su contenuti più familiari per i loro studenti".

Inoltre si fa riferimento alle Indicazioni Nazionali del 2012, che riportano la definizione delle competenze-chiave (Raccomandazione del Parlamento Europeo e del Consiglio del 18 dicembre 2006 - 2006/962/CE), in ambito digitale:

"*La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa implica abilità di base nelle tecnologie dell'informazione e della comunicazione (TIC): l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet*".

2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali

Il comma 124 della Legge n. 107/2015 dispone: "*Nell'ambito degli adempimenti connessi alla funzione docente, la formazione in servizio dei docenti di ruolo è obbligatoria, permanente e strutturale. Le attività di formazione sono definite dalle singole istituzioni scolastiche in coerenza con il piano triennale dell'offerta formativa e con i risultati emersi dai piani di miglioramento delle istituzioni scolastiche previsti dal regolamento di cui al decreto del Presidente della Repubblica 28*

marzo 2013, n. 80, sulla base delle priorità nazionali indicate nel Piano nazionale di formazione adottato ogni tre anni con decreto del Ministro dell'istruzione, dell'università e della ricerca, sentite le organizzazioni sindacali rappresentative di categoria."

Il corpo docente ha partecipato a corsi di formazione nell'ambito di piani nazionali, oltre che ad iniziative organizzate dall'istituzione e possiede generalmente una buona base di competenze e nel caso delle figure di sistema, anche di carattere specialistico. Il percorso complesso della formazione specifica dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica e sull'utilizzo consapevole e sicuro di Internet possono prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva di carattere permanente, legata all'evoluzione rapida delle tecnologie e delle modalità di comunicazione a cui accedono sempre di più ed autonomamente anche i ragazzi.

Anche per il personale Ata saranno estesi momenti di formazione specifica.

2.3. Sensibilizzazione delle famiglie

Le famiglie saranno informate della Policy e di tutte le azioni che essa promuove e ad esse sarà condiviso questo documento all'inizio dell'anno scolastico, unitamente al Patto di corresponsabilità.

Inoltre, potranno consultare, sul sito istituzionale della scuola, materiale relativo all'utilizzo delle TIC, tra cui la piattaforma "Generazioni Connesse".

La scuola avrà cura di sensibilizzare le famiglie attraverso documentazione informativa ed incontri ad un corretto uso delle nuove tecnologie da parte dei ragazzi a casa e a scuola, indicando anche alcune semplici azioni che possono rendere la navigazione sicura. In modo particolare per quanto concerne l'accesso alle attrezzature disponibili in classe (LIM e computer portatile) e nei laboratori informerà sui regolamenti e la normativa vigente. Inoltre promuoverà l'uso delle nuove tecnologie al fine di assicurare un valore aggiunto alla formazione.

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

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 hanno oggi l'obbligo di adeguarsi al cosiddetto GDPR (General Data Protection Regulation) e al D.Lgs. 10 agosto 2018, n. 101.

La scuola osserva il rispetto della privacy dei propri utenti e protegge i dati personali che gli stessi conferiscono all'istituto. I dati personali vengono richiesti solo in caso di effettiva necessità e sono trattati in conformità alla normativa vigente (*Decreto legislativo 30 giugno 2003, n. 196,* c.d. Codice della Privacy). L'utente è sempre informato sulle finalità della raccolta dei dati personali al momento della stessa e ne firma, ove necessario, il consenso al trattamento. I dati personali dell'utente non sono comunicati a terzi senza il consenso dello stesso, fatti salvi i casi previsti dalla legge. Se l'utente decide di fornire alla scuola i propri dati personali, la scuola può comunicarli all'interno dell'Istituto o a terzi, che prestano servizi alla scuola, secondo le modalità previste da normativa vigente.

LIBERATORIA PRIVACY

Per le informative legate alla Privacy e le liberatorie per l'utilizzo delle immagini si rimanda alla sezione Privacy del sito di istituto, raggiungibile da questo link: https://ictoschi.edu.it/privacy

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.

Per garantire che Internet sia uno strumento finalizzato ai soli scopi formativi, verrà esercitato costantemente il monitoraggio e l'aggiornamento dei programmi antivirus e saranno implementati sistemi di filtraggio e di identificazione di contenuti non educativi accessibili on line, certificazioni, blocco di pop-up.

La maggior parte delle aule del nostro Istituto sono dotate di un computer collegato a

LIM/smart TV, ognuno di essi richiede l'inserimento di una password. Ogni docente è tenuto ad un controllo della strumentazione in aula, poiché l'uso del dispositivo non è permesso agli alunni. I computer si collegano alla rete tramite WIFI protetta da password e nota al personale docente, che pertanto è tenuto a:

- non lasciare incustodita e accessibile la propria postazione una volta eseguita la connessione al sistema con le proprie credenziali di autenticazione,
- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a persone non autorizzate, in particolar modo per quanto riguarda l'accesso ad internet e ai servizi di posta elettronica,
- spegnere il PC al termine del lavoro o in caso di assenze prolungate dalla propria postazione.

I computer fissi presenti nelle aule e nei laboratori accedono ad Internet attraverso rete LAN. I portatili collocati nelle aule accedono tramite WIFI. Tutti i computer presenti nella scuola hanno installato un antivirus. I docenti possono accedere con i loro dispositivi personali alla rete WIFI. Gli studenti possono accedere ad Internet in occasione di attività didattiche che si svolgono nel laboratorio informatico.

Si stilano i seguenti punti per regolare l'accesso a internet di tutti i soggetti coinvolti e per garantire questo diritto fondamentale:

Nomina dell'Amministratore di sistema e del Custode delle password:

Il datore di lavoro conferisce all'Amministratore di sistema il compito di sovrintendere alle risorse informatiche dell'Istituto assegnandogli le seguenti attività:

a) gestione dell'hardware e del software (installazione, aggiornamento, rimozione) di tutte le strutture tecniche informatiche dell'istituto, siano esse collegate in rete o meno;

b) configurazione dei servizi di accesso alla rete interna, ad internet e a quelli di posta elettronica con creazione, attivazione e disattivazione dei relativi account;

c) attivazione della password di accensione (BIOS);

d) creazione di un'area condivisa sul server per lo scambio di dati tra i vari utenti, evitando condivisioni dei dischi o di altri supporti configurati nel PC che non siano strettamente necessarie

poiché possono essere un canale per i software che minacciano la sicurezza dell'intero sistema;

e) controllo del corretto utilizzo delle risorse di rete, dei computer e degli applicativi, durante le normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

f) rimozione sia sui PC degli incaricati sia sulle unità di rete, di ogni tipo di file o applicazione che può essere pericoloso per la sicurezza o costituisce violazione del presente regolamento;

g) distruzione delle unità di memoria interne alla macchina (hard - disk, memorie allo stato solido) ogni qualvolta si procederà alla dismissione (procedura discarico inventariale) di un PC e dei supporti removibili consegnati a tale scopo dagli utenti;

h) utilizzo delle credenziali di amministrazione del sistema per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di indispensabile ed indifferibile necessità di intervento per prolungata assenza, irrintracciabilità o impedimento dello stesso, solo per il tempo necessario al compimento di attività indifferibili e solo su richiesta del Responsabile del trattamento.

L'Amministratore di sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, e dopo aver richiesto l'autorizzazione all'utente interessato, al PC di ciascun utente. Il Custode delle password è incaricato di custodire e conservare in luogo riservato e sicuro, in formato cartaceo, le credenziali; è altresì tenuto a ottemperare al suo compito avendo cura di non diffondere, nemmeno accidentalmente, le stesse a persone estranee al loro utilizzo.

3.3. E-mail

L'account di posta elettronica è solo quello istituzionale utilizzato ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita. La posta elettronica è protetta da antivirus, e quella certificata anche dall'antispam. La corrispondenza privata non deve essere inviata da e per gli account di servizio. Gli utenti sono responsabili dell'uso dell'account loro assegnato e sono tenuti ad utilizzarlo in modo conforme a quanto stabilito dal presente regolamento, quindi devono:

a) conservare la password nella massima riservatezza e con la massima diligenza,

b) mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti,

c) utilizzare l'account per l'invio di comunicazioni attinenti all'attività lavorativa e di studio

d) al termine delle operazioni effettuare il logout dall'account.

Agli utenti è fatto divieto di qualsiasi uso della posta elettronica che possa in qualche modo recare danno all'istituto o a terzi e quindi di:

a) prendere visione della posta altrui,

b) simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza,

c) utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'istituto,

d) trasmettere a mezzo posta elettronica dati sensibili, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati,

e) utilizzare il servizio di posta elettronica per inoltrare contenuti e altre e-mail che non siano di lavoro o a fini di studio.

Tutti i docenti e gli alunni possiedono un account *Google Workspace For Education*. La nostra scuola infatti, ha attivato la piattaforma Classroom.

3.4 Sito web della scuola

Il sito *web* della scuola è gestito dalla Segreteria, da un docente referente e dall'Animatore Digitale; i genitori ad inizio anno scolastico esprimono o meno il proprio consenso all'utilizzo di foto e notizie relative agli alunni per l'aggiornamento del sito e per altre finalità. In nessun caso l'Istituto potrà essere ritenuto responsabile dei danni di qualsiasi natura causati direttamente o indirettamente dall'accesso al sito, dall'incapacità o impossibilità di accedervi, dall'affidamento dell'utente e dall'utilizzo dei contenuti. L'Istituto provvederà ad inserire nel sito informazioni e comunicazioni aggiornate, servizi, notizie, eventi, articoli relativi alle attività didattiche dell'Istituto, documenti e albo, contatti e orari.

Sono previste, inoltre, piattaforme virtuali di condivisione di materiali come *Google Classroom*, e altre, previa comunicazione e informazione alla famiglia.

Dal sito istituzionale è possibile accedere al Registro Elettronico. Ogni docente accede al

registro elettronico attraverso una password personale che non può essere comunicata a terzi.
Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, nel quale il corpo docente è tenuto a registrare assenze, valutazioni, note, argomenti delle lezioni e compiti. L'uso del registro elettronico è spiegato alle famiglie nel corso del primo Consiglio di classe dell'anno scolastico. Attraverso il registro è anche possibile la condivisione di materiali tra i docenti e con gli studenti.

3.5. Social network

La scuola non utilizza social network per la didattica.

3.6. Utilizzo di supporti magnetici

Tutto il personale è invitato a non utilizzare dispositivi di memoria esterna (chiavi USB, CD, DVD, ecc.) ma ad utilizzare i Repository su Cloud del dominio @ictoschi.edu.it.

Qualora sia indispensabile l'utilizzo di supporti magnetici, gli utenti devono averne particolare cura (Disposizioni anticipate di trattamento, chiavi USB, CD riscrivibili…) in particolar modo quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati qui contenuti. Di conseguenza le azioni da compiere obbligatoriamente sono le seguenti:

a) porre attenzione nell'utilizzo dei supporti rimovibili personali;

b) custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto;

c) consegnare i supporti magnetici riutilizzabili (DAT, chiavi USB, CD riscrivibili, Hard Disk esterni ...) obsoleti all'Amministratore di sistema per l'opportuna distruzione onde evitare che il loro contenuto possa essere successivamente recuperato in seguito alla cancellazione;

d) criptare l'accesso ai dispositivi personali (PC, Hard Disk esterni, USB, ecc…) con password sicura e non divulgazione della stessa.

3.7. Utilizzo delle stampanti e dei materiali d'uso

Stampanti e materiali di consumo in genere (carta, inchiostro, toner, supporti digitali come CD e DVD) possono essere usati esclusivamente per compiti di natura strettamente istituzionale, evitando in ogni modo sprechi e utilizzi eccessivi. Gli utenti devono effettuare la stampa dei dati solo se strettamente necessaria e ritirare prontamente dai vassoi delle stampanti comuni i fogli per impedire a persone non autorizzate di accedere alle stampe di documenti riservati, distruggere personalmente e sistematicamente le stampe che non servono più.

3.8. BYOD Regolamento per l'utilizzo dei dispositivi digitali personali a scuola

L'azione del PNSD "Politiche attive per il BYOD" (*Bring your own device*), - letteralmente: porta il tuo dispositivo - punta a garantire a tutti gli studenti una formazione digitale che parta dal saper usare i propri dispositivi. Si legge testualmente "La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (*Bring Your Own Device*), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficientemente integrato". Poiché la tecnologia fornisce agli studenti opportunità innovative ed inedite per incrementare la loro cultura, in linea con quanto specificato nel PNSD, il nostro Istituto intende favorire tale processo garantendone la sicurezza attraverso una modalità di interazione che contribuisca al miglioramento dell'ambiente educativo e di apprendimento. Pertanto l'uso improprio dei dispositivi digitali mobili a scuola è inaccettabile e viene sanzionato in misura della gravità in base a quanto stabilito dal Regolamento di Istituto.

1. Dispositivi ammessi: notebook con installato il browser Chrome, Chromebook, tablet con installato il browser Chrome, fotocamera digitale, lettori e registratori audio e/o video.

2. I dispositivi devono essere usati a scuola per soli scopi didattici e solo dopo previa autorizzazione esplicita dell'insegnante (regola del semaforo). Agli studenti non è permesso usarli per giochi o attività diverse da quelle didattiche durante le ore scolastiche o durante le pause ricreative.

3. È vietato agli studenti usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare media o fare foto in classe senza il permesso dell'insegnante e senza il consenso della persona che viene registrata.

4. Audio e video registrati a scuola a fini didattici possono essere pubblicati esclusivamente in canali di comunicazione intestati ufficialmente all'I.C. Toschi.

5. Gli studenti sono responsabili personalmente dei propri dispositivi; è vietato prendere in prestito dispositivi di altri studenti.

6. La scuola non è responsabile della sicurezza dei dispositivi e di eventuali danni agli stessi.

7. Gli studenti sono responsabili di riportare a casa il dispositivo al termine delle lezioni. La scuola non sarà ritenuta responsabile per nessun dispositivo degli studenti lasciato a scuola.

8. Uso non consentito di Internet:

a. Usare Internet per scopi diversi da quelli didattici;

b. Scaricare musica, video e programmi da internet o qualsiasi file senza il consenso dell'insegnante;

c. Giocare sul computer, in rete o diversamente (se non come parte di una lezione);

d. Usare dispositivi audio, video o fotografici per ritrarre qualsiasi persona durante l'attività didattica per scopi diversi da quelli didattici, se non ha ottenuto il permesso esplicito del docente e se non ha autorizzato tale attività.

9. Agli studenti è richiesto di caricare completamente le batterie del proprio dispositivo a casa e devono essere consapevoli che:

a. non sarà possibile ricaricare i dispositivi durante l'orario di lezione;

b. non sarà possibile ricaricare i dispositivi in aula; a tal scopo si consiglia di dotarsi di caricabatteria portatili e di portare il dispositivo completamente carico a scuola.

10. Diritti di proprietà intellettuale:

Gli studenti devono rispettare e proteggere la proprietà intellettuale altrui:

- Non è ammessa la copia o il plagio di qualsiasi materiale;
- Non è ammessa la violazione dei copyrights;
- Si deve attribuire, citare e richiedere il permesso degli autori o creatori delle informazioni o dei media originali (se richiesto dalla legge o da accordo).

11. Diritto di ispezione:

- La scuola si riserva il diritto di monitorare le attività online degli utenti.
- La scuola, in accordo con la famiglia, può ispezionare la memoria del dispositivo dello studente se ritiene che le regole scolastiche non siano state rispettate, questo comprende, ma non è limitato, registrazioni audio e video, fotografie scattate nelle pertinenze scolastiche e che violano la privacy altrui, o ogni altra questione legata a cyberbullismo, ecc…

12. Sanzioni per il mancato rispetto del Regolamento: l'accesso al network della scuola è un privilegio, non un diritto. L'uso della tecnologia, sia essa proprietà della scuola o un dispositivo fornito dagli studenti, comporta responsabilità personali. Ci si aspetta che gli studenti rispettino le regole dell'I.C., agiscano responsabilmente e onorino i termini e le condizioni fissate dall'insegnante di classe e dalla scuola. Il mancato rispetto di questi termini e condizioni potrà risultare nella temporanea perdita di accesso alla rete nonché altre azioni disciplinari e legali, se necessario. Gli studenti saranno ritenuti responsabili delle loro azioni e sono incoraggiati a segnalare immediatamente ogni uso accidentale al loro insegnante. Le sanzioni dipenderanno dalla gravità dell'accaduto e sanzionate secondo il Regolamento di Istituto. I dispositivi potranno essere confiscati per l'intera giornata scolastica.

ISTITUTO COMPRENSIVO "G.B. TOSCHI" BAISO - VIANO
Dirigenza e segreteria: Via Ca' Toschi 4 - 42031 Baiso (RE)
C.F. 80015710355 – tel. 0522/993571-993572 – Sito Web: www.ictoschi.edu.it
Mail: reic819003@istruzione.it – reic819003@pec.istruzione.it

Oggetto: PATTO BYOD (*Bring Your Own Device* - Porta il tuo dispositivo)

Carissimo/a alunno/a, come studente/essa della classe..... Sez. ……. del plesso..... avrai la possibilità di poter portare da casa a scuola il tuo device. Questa opportunità comprende anche alcune regole.

Leggi bene il seguente patto perché, se non rispetterai queste regole, ti verrà tolta tale possibilità.

1. Non sei obbligato a portare a scuola il tuo device.

2. I tuoi genitori devono essere informati dell'utilizzo del dispositivo a scuola.

3. Il device personale verrà utilizzato a scuola solo quando richiesto dagli insegnanti.

4. La tipologia di device sarà preventivamente concordata con l'insegnante.

5. Utilizzerai il device esclusivamente per scopi didattici, seguendo il regolamento della scuola e le indicazioni degli insegnanti.

6. Ricorda che il BYOD è un privilegio che può essere revocato.

7. Se userai impropriamente il device, ti verrà ritirato.

8. Non puoi utilizzare i dispositivi nei bagni, negli spogliatoi, nei corridoi, durante gli spostamenti e l'intervallo e, comunque, in ogni situazione se non autorizzato dagli insegnanti.

9. Collega sempre il tuo dispositivo alla rete wi-fi della scuola per navigare in un ambiente protetto.

10. Se porti il tuo dispositivo, devi assicurarti che sia carico.

11. Il tuo dispositivo è sotto la tua responsabilità, usalo solo per scopi didattici, conservalo in sicurezza, utilizzalo rispettando le regole dei tuoi genitori e della scuola.

12. Utilizza il tuo dispositivo in modo significativo e opportuno dal punto di vista didattico e rispettoso delle leggi europee e dello Stato.

13. Rispetta le regolamentazioni sulla Privacy e i diritti delle persone che ti circondano.

ROSSO All'inizio della lezione i dispositivi devono essere spenti; no silenzioso; no vibrazione.

GIALLO I dispositivi devono essere messi a lato del banco. Devono essere in modalità silenziosa o vibrazione. I dispositivi possono essere toccati solo con il consenso dell'insegnante.

VERDE Gli studenti possono tenere sul banco i dispositivi e usarli quando vogliono nel rispetto delle regole e della finalità didattica. Gli studenti devono tenere i dispositivi in modalità silenziosa.

Per consenso e accettazione.

Luogo e data: _____ Firma dell'alunno/a Firma dei genitori/tutori

DICHIARAZIONI DEI GENITORI/TUTORI LEGALI

I sottoscritti _____ e _____ tutori legali dell'alunno/a _____ frequentante la classe _____ sez. ____ della scuola _____

DICHIARANO:

1. di essere al corrente che, in ambito scolastico, i docenti potranno introdurre, a fianco degli strumenti e dei materiali didattici in uso a scuola, l'utilizzo di applicazioni, contenuti e servizi fruibili in locale e in Internet tramite dispositivi elettronici propri;

2. di collaborare con i docenti nel responsabilizzare i ragazzi sulle modalità di accesso a Internet e sulle regole a cui attenersi;

3. che durante la permanenza a scuola del dispositivo il/la proprio/a figlio/a sarà il/la solo/a responsabile della sua custodia e del suo uso corretto, secondo le regole e le disposizioni concordate con gli insegnanti.

AUTORIZZANO IL/LA PROPRIO/A FIGLIO/A a portare a scuola il proprio device* secondo la modalità e la tipologia concordata con l'insegnante.

Luogo e data _____ Firma dei genitori/tutori legali _____

***I device consentiti a scuola sono notebook con installato il browser Chrome, chromebook, tablet con installato il browser Chrome, fotocamera digitale, lettori e registratori audio e/o video.**

3.9 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.

Gli strumenti utilizzati per la comunicazione online sono: il registro elettronico, la mail, le Google Workspace per l'apprendimento di @ictoschi.edu.it (dominio applicativo) e programmi autorizzati dai genitori e normati dalla legge sulla Privacy vigente.

Il registro elettronico permette la comunicazione con le famiglie sull'andamento scolastico, i colloqui, gli eventi, i risultati scolastici e comunicazioni varie.

È importante ricordare che l'art. 22 del CCNL 2016/2018 (diritto alla disconnessione), fornisce i criteri generali per l'utilizzo di strumentazioni tecnologiche in orario diverso da quello di servizio per conciliare al meglio vita lavorativa e familiare.

Il nostro piano d'azioni

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

- Effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse.
- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola.
- 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).

Azioni da sviluppare a livello di istituzione scolastica

Il monitoraggio e l'implementazione delle stesse sarà competenza del Team Digitale e dello staff direttivo in fase di aggiornamento annuale.

- Organizzare uno o più eventi o attività volti a consultare i docenti dell'Istituto per redigere o integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione degli studenti/studentesse su indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- Organizzare incontri per la consultazione dei genitori su indicazioni/regolamenti sull'uso dei dispositivi digitali personali.
- 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 gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali.
- Organizzare uno o più eventi o attività volti a formare i genitori 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).
- Attivazione di iniziative di formazione in particolare rivolte allo sviluppo e alla diffusione del Coding e del pensiero computazionale.
- Monitoraggio del piano digitale d'istituto e dei risultati conseguiti.

4 Strumentazione personale

Facendo riferimento al Patto educativo di corresponsabilità scuola-famiglia, integrato con delibera del Consiglio di Istituto in data 07/09/2020 si ricorda, tra l'altro, il compito della famiglia di:

- Educare la studentessa/studente ad utilizzare i dispositivi digitali nel rispetto dei regolamenti dell'Istituto, solo per fini didattici e su autorizzazione esplicita e motivata dell'insegnante;
- Educare la studentessa/studente a segnalare agli insegnanti e ai genitori episodi di bullismo o cyberbullismo di cui fosse vittima o testimone;
- Educare la studentessa/studente ad accettare, rispettare e aiutare gli altri, impegnandosi a comprendere le ragioni dei comportamenti altrui, evitando di utilizzare gli strumenti digitali e i mezzi di comunicazione per aggredire, denigrare ingiuriare e molestare altre persone, consapevoli che certi comportamenti si configurano come reati perseguibili dalla Legge;

Si ricorda inoltre la successiva integrazione dei profili afferenti alla Didattica Digitale Integrata nella quale la famiglia si impegna a:

- vigilare affinché i propri figli non assumano condotte lesive dell'onore e del decoro, nonché della privacy degli insegnanti e dei compagni.

4.1. Per gli studenti: gestione degli strumenti personali - cellulari, tablet ecc.

In ambito scolastico è consentito l'uso di dispositivi elettronici solo per fini didattici. L'utilizzo dei dispositivi deve essere in ogni caso autorizzato dai docenti.

Al di fuori dell'utilizzo strettamente collegato allo svolgimento delle attività didattiche è vietato l'uso di tutti i dispositivi elettronici compresi i telefoni cellulari ed i dispositivi per ascoltare musica.
È consentito agli alunni in difficoltà, con DSA e BES di utilizzare il proprio tablet o notebook con il controllo del docente.
Per quanto riguarda la gestione degli strumenti personali (cellulari, tablet, etc.) da parte degli studenti, dei docenti e di tutto il personale della scuola, si rinvia a quanto previsto dal Regolamento d'Istituto e dal patto di corresponsabilità scuola famiglia nell'integrazione specifica.

4.2. Per i docenti: gestione degli strumenti personali - cellulari, tablet ecc...

Durante le ore delle lezioni non è in alcun caso consentito l'utilizzo del cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.

L'accesso alla rete WIFI dell'Istituto è disponibile per i docenti e protetta da password.

4.3.Per il personale della scuola: gestione degli strumenti personali - cellulari, tablet ecc.

Durante l'orario di servizio al restante personale scolastico non è in alcun modo consentito l'utilizzo del cellulare.

5. Prevenzione, rilevazione e gestione dei casi

5.1. Rischi

Al personale che opera nella scuola, e in modo particolare agli insegnanti, viene oggi offerta la possibilità di essere promotori e garanti della costruzione dialogica di un percorso formativo partecipato, ma il loro ruolo diventa spesso inevitabilmente quello di confidenti degli alunni e delle loro esperienze. Proprio per questo, gli insegnanti sono anche investiti del ruolo di una sorta di torre di avvistamento, avamposto privilegiato delle problematiche e dei rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno.

La prima responsabilità degli insegnanti consiste, dunque, nell'imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Tra questi, un'attenzione specifica andrà prestata ai fenomeni di bullismo/cyberbullismo, sexting e adescamento o grooming.

5.2. Azioni

L'obiettivo che l'insegnante deve proporsi dopo avere riconosciuto il pericolo è agire di conseguenza, con azioni di contrasto efficaci e mirate, rispetto ai rischi sopra elencati.
Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli alunni in orario scolastico, vi sono le seguenti:

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo materiali messi a disposizione sul sito del progetto "Generazioni connesse";
- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli studenti in orario scolastico;
- dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list);
- bloccare l'accesso a un sito o a un insieme di pagine impedendone la consultazione;

- controllare periodicamente i siti visitati dagli alunni;
- utilizzare un software in grado di intercettare le richieste di collegamento e di respingere quelle non conformi alle regole stabilite dall'amministratore;
- affidare a un gruppo di docenti scelto le regole di filtraggio.

A tal proposito, la scuola proporrà incontri formativi atti a favorire momenti di riflessione e attività laboratoriali.

5.3. Che 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 al referente per l'area di competenza ed al Dirigente Scolastico.

Questa sezione dell'e-Policy 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.

Le procedure sono passibili di costanti aggiornamenti e modifiche in termini di miglioramento delle stesse e nel rispetto della normativa vigente.

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'individuazione 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.

Si considerano da segnalare tutte quelle situazioni caratterizzate da *volontarie e ripetute aggressioni* mirate a insultare, minacciare, diffamare e/o ferire una persona (o un piccolo gruppo) tramite un utilizzo irresponsabile dei social network.
In particolare si segnaleranno:

- contenuti afferenti la violazione della privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà, di eventi privati, ecc.);
- contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti, che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, ecc.);
- contenuti afferenti alla sessualità: messaggi molesti, conversazioni (testo o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), ecc…

Tutte le segnalazioni riportate dai docenti verranno registrate su apposita scheda (in coda al documento).

5.4. Come segnalare: quali strumenti e a chi

L'insegnante riveste la qualifica di pubblico ufficiale in quanto l'esercizio delle sue funzioni non

è solo 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 del team di riferimento.

Gli insegnanti, anche con l'ausilio tecnico dell'Animatore digitale, possono provvedere a conservare le prove della condotta incauta, scorretta o dell'abuso rilevate sui pc della scuola: soprattutto la data e l'ora, il contenuto dei messaggi e, se possibile, l'ID del mittente (es. username, mail, numero di telefono cellulare) o l'indirizzo web del profilo ed il suo contenuto. Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono ogni messaggio, voce/testo/immagine, conservando così il numero del mittente.

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

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

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

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

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

In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.

Per i reati più gravi (es. pedopornografia) l'Istituzione scolastica ha l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).

Inoltre ci si potrà avvalere dei due servizi messi a disposizione dal Safer Internet Center il "*Clicca e Segnala*" di Telefono Azzurro e "*STOP-IT*" di Save the Children.

Una volta ricevuta la segnalazione, infatti, gli operatori procederanno a coinvolgere le autorità competenti in materia.

5.5. Gestione dei casi

Le procedure interne per la rilevazione e la gestione dei casi, nonché la segnalazione alla Dirigenza Scolastica ed eventualmente alle autorità competenti, avvengono secondo i protocolli suggeriti dalla piattaforma messa a disposizione da "Generazioni Connesse", come da schemi allegati.

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

1. 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.

2. 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, si prega di fare 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.

Studenti e studentesse hanno a disposizione, inoltre, i seguenti strumenti:

- docenti referenti per sportello di ascolto, con professionisti specifici per appuntamenti;
- docente referenti per le segnalazioni in merito a bullismo/cy

Per quanto riguarda la necessità di segnalazione e rimozione di contenuti online lesivi, ciascun minore (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.

Ci si può inoltre rivolgere ai seguenti servizi:

- ✓ Helpline di Generazioni Connesse (numero verde: 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.

In caso di rischi online… cosa fare?

Intervenire: sì o no?

SEMPRE. Ricorda che il tuo compito è educativo e generativo: sei chiamato/a garantire il benessere dei tuoi alunni, oltre che a trasmettere conoscenze.

Se un tuo/a alunno/a **ti ha confidato qualcosa che lo/a preoccupa di ciò che accade online, significa che si fida di te e pensa che tu abbia le risorse per aiutarlo/a.**

Vediamo insieme quali possono essere le risorse che hai a disposizione per aiutarlo/a e come attivarle.

Intervenire come? Creare rete

Non sei solo/a. Se sospetti che un tuo/a alunno/a possa essere vittima o responsabile di una

situazione di cyberbullismo, sexting o vittima di adescamento online, ricordati che **nell'affrontare quanto accade non sei solo/a.**

Non pensare a risolvere la situazione con tempestività, ma fermati a riflettere innanzitutto a come ridare benessere al tuo/a alunno/a che sta vivendo la situazione di disagio.

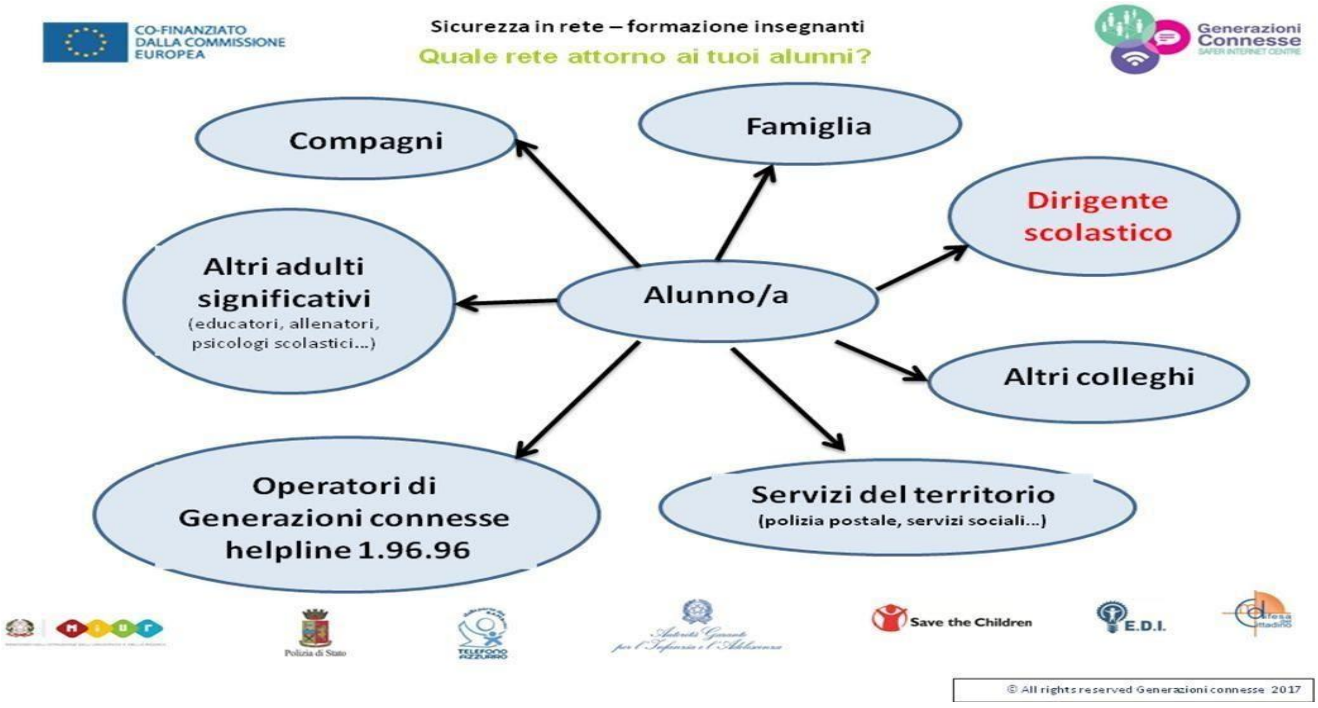
Lo/la conosci, fermati a pensare di cosa hai bisogno per aiutarlo e confrontati su come poter intervenire nel modo migliore.

I **passi imprescindibili** sono:

1. **Ascolta:** chiedigli/le cosa puoi fare per lui/lei e cosa desidera che accada;
2. **Coinvolgi:** sicuramente il tuo Dirigente Scolastico. Valutate poi insieme con quali altri persone parlare di quanto sta accadendo;
3. **Intervenite**: agite per ridare benessere al tuo/a alunno/a.

- **Il primo passo per intervenire è: chi posso coinvolgere per decidere come intervenire?**

Chiediti chi sono le persone attorno al tuo/a alunno/a con cui puoi parlare. Qui sotto trovi uno schema sintetico che ti può aiutare in questa riflessione:



- ✓ **Il secondo passo per intervenire è: decidere come**

Posto il fatto che a decidere come intervenire non sei solo/a (vedi sopra), non resta che decidere come gestire la situazione di cui sei venuto/a a conoscenza.

I tuoi alunni non sono tutti uguali: ciascuno ha caratteristiche peculiari proprie. Un buon intervento

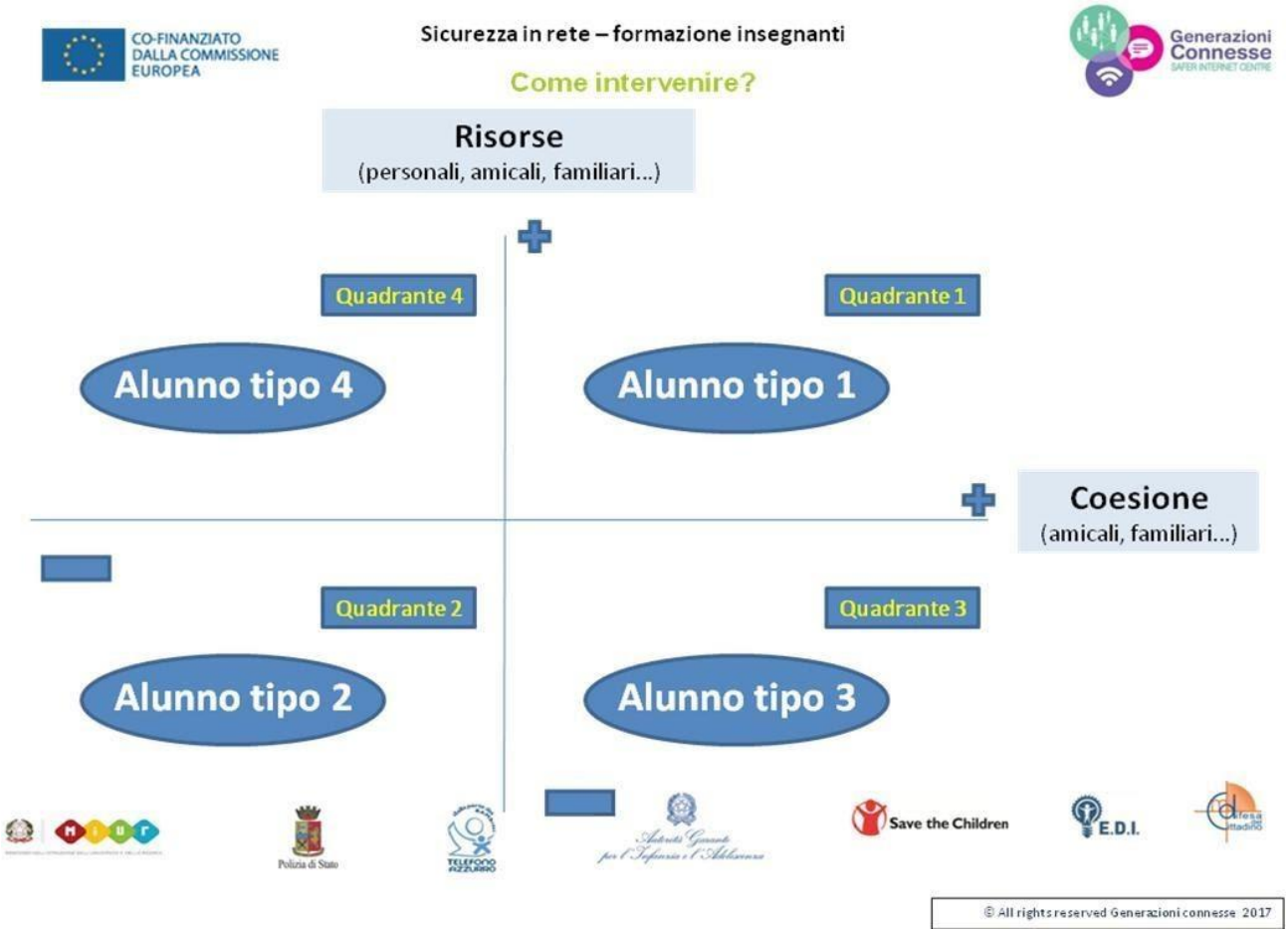
tiene conto di:

A - le caratteristiche di unicità del tuo/a **alunno**/a coinvolto/a nella situazione di difficoltà; B - il tipo di **famiglia** da cui proviene

C - la **classe** in cui sei

D – la **Comunità** scolastica

Qui sotto trovi uno schema sintetico che ti può aiutare a decidere come intervenire.



Alunno tipo 1

Sono gli alunni con alte risorse individuali, con una famiglia presente e con un gruppo di amici che lo/a stima e gli/le vuole bene.

In questi casi è auspicabile che per intervenire nella situazione che si è venuta a creare, oltre al dirigente scolastico tu possa coinvolgere nella creazione di una rete supportiva sia la famiglia che gli amici. Per decidere chi coinvolgere e come intervenire, ricordati che puoi chiedere un confronto o un consiglio anche agli operatori di Generazioni Connesse presenti nella tua scuola o rivolgerti alla helpline del progetto, al numero 1.96.96.

Alunno tipo 2

Sono gli alunni con poche risorse personali, con famiglie poco presenti e senza una rete di amici.

In questi casi è auspicabile che per intervenire nella situazione che si è venuta a creare, oltre al dirigente scolastico tu possa coinvolgere/attivare una rete extra scolastica, di servizi e istituzioni. Per decidere chi coinvolgere e come intervenire, ricordati che puoi chiedere un confronto o un consiglio anche agli operatori di Generazioni Connesse presenti nella tua scuola o rivolgerti alla helpline del progetto, al numero 1.96.96.

Alunno tipo 3

Sono gli alunni con poche risorse personali, con famiglie poco presenti ma con una buona rete di amici. In questi casi è auspicabile che per intervenire nella situazione che si è venuta a creare, oltre al dirigente scolastico tu possa coinvolgere il gruppo di amici, chiedendo al gruppo di amici di aiutare e supportare il compagno in difficoltà (alleanza classe-scuola). È comunque importante coinvolgere la famiglia, ma nella consapevolezza che forse non ha le risorse per affrontare da sola quanto sta accadendo.

Per decidere chi coinvolgere e come intervenire, ricordati che puoi chiedere un confronto o un consiglio anche agli operatori di Generazioni Connesse presenti nella tua scuola o rivolgerti alla helpline del progetto, al numero 1.96.96.

Alunno tipo 4

Sono gli alunni con buone risorse personali, ma spesso un po' soli.

In questi casi è auspicabile che per intervenire nella situazione che si è venuta a creare, oltre al dirigente scolastico tu possa lavorare in stretta sinergia con il tuo/a alunno/a (alleanza alunno/a-scuola). È comunque importante coinvolgere la famiglia, ma nella consapevolezza che forse non ha le risorse per affrontare da sola quanto sta accadendo.

Per decidere chi coinvolgere e come intervenire, ricordati che puoi chiedere un confronto o un consiglio anche agli operatori di Generazioni Connesse presenti nella tua scuola o rivolgerti alla helpline del progetto, al numero 1.96.96.

Come tenere traccia dell'intervento?

È importante tenere traccia di quanto accade e del tipo di intervento che viene messo in atto, per creare una lista di **buone prassi** che **vadano a comporre uno storico di quanto viene attivato a scuola per garantire il benessere online dei propri alunni.**

Gli strumenti per segnalare e monitorare i casi a scuola

Qui di seguito puoi trovare due strumenti che ti potranno agevolare

1. nell'effettuare la segnalazione: è consigliabile dotarsi di un **modulo**, affinché le segnalazioni vengano effettuate per iscritto e contengano tutte le informazioni necessarie alla presa in carico della situazione.
2. nel tenere traccia di ciò che è avvenuto rispetto ai comportamenti dei tuoi alunni online e di come è stato gestito.

L'obiettivo a lungo termine che come comunità scolastica potete darvi a questo proposito è quello di creare una memoria condivisa non solo di ciò che accade nella tua scuola rispetto al web, ma anche di strutturare una fonte esemplificativa che possa orientare sempre più e sempre meglio le azioni di contrasto ad episodi che, nel tempo, potrebbero ripetersi.

Utilizza il **diario di bordo** per tenere traccia di ciò che è avvenuto rispetto ai comportamenti dei tuoi alunni online e di come è stato gestito.

Co-financed by the European Union
Connecting Europe Facility

Generazioni Connesse

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi
Scuola_____ Anno Scolastico_____

N°	Data	ora	Episodio *(riassunto)*	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		

© All rights reserved Generazioni connesse 2017

MODULO PER LA SEGNALAZIONE DI CASI

ISTITUTO COMPRENSIVO "G.B. TOSCHI" BAISO - VIANO
Dirigenza e segreteria: Via Ca' Toschi 4 - 42031 Baiso (RE)
C.F. 80015710355 – tel. 0522/993571-993572 – Sito Web: www.ictoschi.edu.it
Mail: reic819003@istruzione.it – reic819003@pec.istruzione.it

Descrizione dell'episodio o del problema		
Soggetti coinvolti	Vittima/e:	Classe:
	1.	
	2.	
	3.	
	Bullo/i:	Classe:
	1.	
	2.	
	3.	
Chi ha riferito dell'episodio?	- La vittima	
	- Un compagno della vittima, nome:	
	- Genitore, nome:	
	- Insegnante, nome:	
	- Altri, specificare:	
Atteggiamento del gruppo	Da quanti compagni è sostenuto il bullo? Quanti compagni supportano la vittima o potrebbero farlo?	
Gli insegnanti sono intervenuti in qualche modo?		
La famiglia o altri adulti hanno cercato di intervenire?		
Chi è stato informato della situazione?	❑ **coordinatore di classe**	data:
	❑ consiglio di classe	data:
	❑ dirigente scolastico	data:
	❑ la famiglia della vittima/e	data:

	❑ la famiglia del bullo/i	data:
	❑ le forze dell'ordine	data:
	❑ altro, specificare:	

MODULO PER IL FOLLOW-UP DEI CASI

	AZIONI INTRAPRESE	La situazione è…
Aggiornamento 1		❑ migliorata ❑ invariata ❑ peggiorata Come:
Aggiornamento 2		❑ migliorata ❑ invariata ❑ peggiorata Come:
Aggiornamento 3		❑ migliorata ❑ invariata ❑ peggiorata Come:

5.6. 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.

RIFERIMENTI

SPORTELLO SOCIALE DI SCANDIANO
Indirizzo: via Reverberi 1, al secondo piano
tel.: 0522985860 e 0522985866 dal lunedì al sabato, fra le 7,30 e le 9,30 Ricevimento al pubblico:
martedì, giovedì e venerdì dalle 9,30 e le 13,00
lunedì, mercoledì e sabato CHIUSO

AZIENDE SANITARIE LOCALI
I riferimenti per contattare le aziende sanitarie della propria città si trovano al seguente link:
http://salute.regione.emilia-romagna.it/ssr/aziende-sanitarie-irccs/erogazione-dellassistenza aziende-sanitarieirccs-asp

Uffici Relazioni col pubblico distrettuali:
URP Arcispedale S. Maria Nuova - urp.santamarianuova@ausl.re.it
Tel. centralino: 0522.335111

URP Reggio Emilia - urp.reggioemilia@ausl.re.it
URP Scandiano - urp.scandiano@ausl.re.it

Le competenze erogate da questi servizi consistono nell'ottenere un sostegno psicologico, psichiatrico o neuropsichiatrico sulle problematiche psicologiche, anche associate all'uso di Internet e a tutti i tipi di comportamenti a rischio e che configurino un reato.

GARANTE REGIONALE PER L'INFANZIA E L'ADOLESCENZA
Viale Aldo Moro, 50 40127 Bologna, tel. 051. 5276263 - 051. 5275713 garanteinfanzia@regione.emilia-romagna.it
www.assemblea.emr.it/garanti/attivita-e-servizi/infanzia

Competenze/Servizi: Segnala all'autorità giudiziaria i servizi sociali e competenti; accoglie le segnalazioni di presunti abusi; fornisce informazioni sulle modalità di tutela e di esercizio di questi diritti; segnala alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate, sempre per tutti i comportamenti a rischio e che configurino un reato.

UFFICIO SCOLASTICO REGIONALE
Via de' Castagnoli, 1 40126 – Bologna. Tel: 051. 37851
direzione-emiliaromagna@istruzione.it
www.istruzioneer.it/

Competenze/Servizi: Tra le varie funzioni, supporta la scuola in attività di prevenzione. Può affiancare le scuole nei casi di segnalazione di comportamenti a rischio correlati all'uso di internet e per i comportamenti a rischio e che configurino un reato relativi al cyberbullismo.

TRIBUNALE PER I MINORENNI
Via del Pratello, 36 40122 – Bologna. Tel: 051. 2964880
tribmin.bologna@giustizia.it
http://www.tribmin.bologna.giustizia.it/

Competenze/Servizi: Tra le varie attività si occupa di tutti i procedimenti che riguardano reati, misure rieducative, tutela e assistenza, sempre per tutti i comportamenti a rischio e che configurino un reato.

POLIZIA POSTALE E DELLE COMUNICAZIONI
Via Francesco Zanardi, 28/6 – Bologna. Tel: 051. 6352611
poltel.bo@poliziadistato.it
www.commissariatodips.it/

Competenze/Servizi: Si occupa di accogliere tutte le segnalazioni o denunce relative a comportamenti a rischio nell'utilizzo di internet sempre per tutti i comportamenti a rischio e che configurino un reato, quali: furto di identità, cyberbullismo (nel caso di cyberstalking), commercio on-line (nel caso di clonazione di carta di credito), pedopornografia on-line, grooming (adescamento on-line), gioco d'azzardo on-line, sexting.

5.7. Allegati e procedure

PROCEDURE INTERNE: COSA FARE IN CASO DI SOSPETTO DI CYBERBULLISMO?

1. Il docente che ha il sospetto che stia accadendo nella propria classe un episodio di cyberbullismo avvisa il referente per il cyberbullismo e valuta con lui le strategie di intervento; di concerto avvisano il Dirigente Scolastico.
2. Monitora la situazione della classe e cerca di capire il livello di diffusione nell'Istituto.
3. Parla in classe del cyber bullismo, di ciò che dice la legge italiana (L. 71/2017), delle sue conseguenze e informa gli studenti che possono segnalare al gestore del sito internet o al garante della privacy eventuali contenuti offensivi/lesivi che li riguardano.
4. Se hai dei dubbi consulta l'helpline di Generazioni Connesse (19696) e ricorda agli studenti che possono farlo anche loro (anche tramite chat).

PROCEDURE INTERNE: COSA FARE IN CASO DI EVIDENZA DI CYBERBULLISMO?

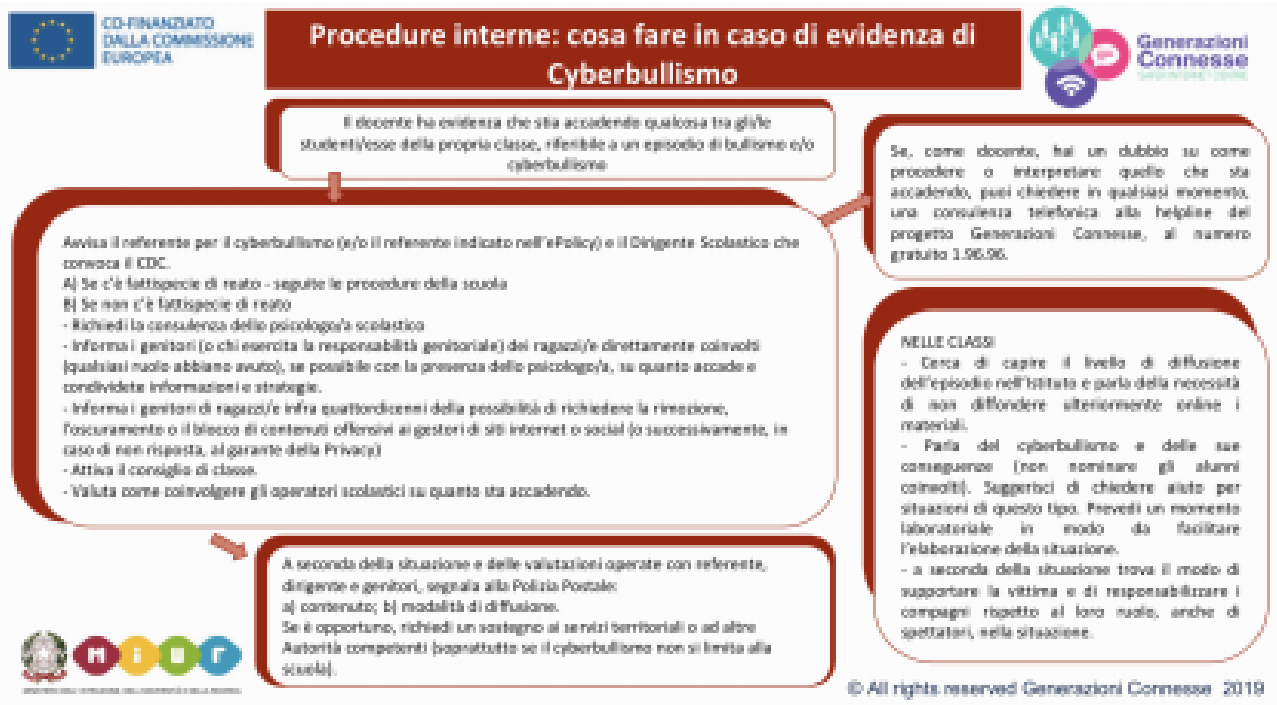
Il docente ha evidenza che stia accadendo nella propria classe un episodio di cyberbullismo. Avvisa il referente per il cyberbullismo e il Dirigente Scolastico.

1. Se c'è fattispecie di reato si seguono le procedure della scuola.

   Possibilità di richiedere la rimozione, l'oscuramento o il blocco di contenuti offensivi ai gestori di siti internet; valuta come coinvolgere gli operatori scolastici.

2. Se non c'è fattispecie di reato:

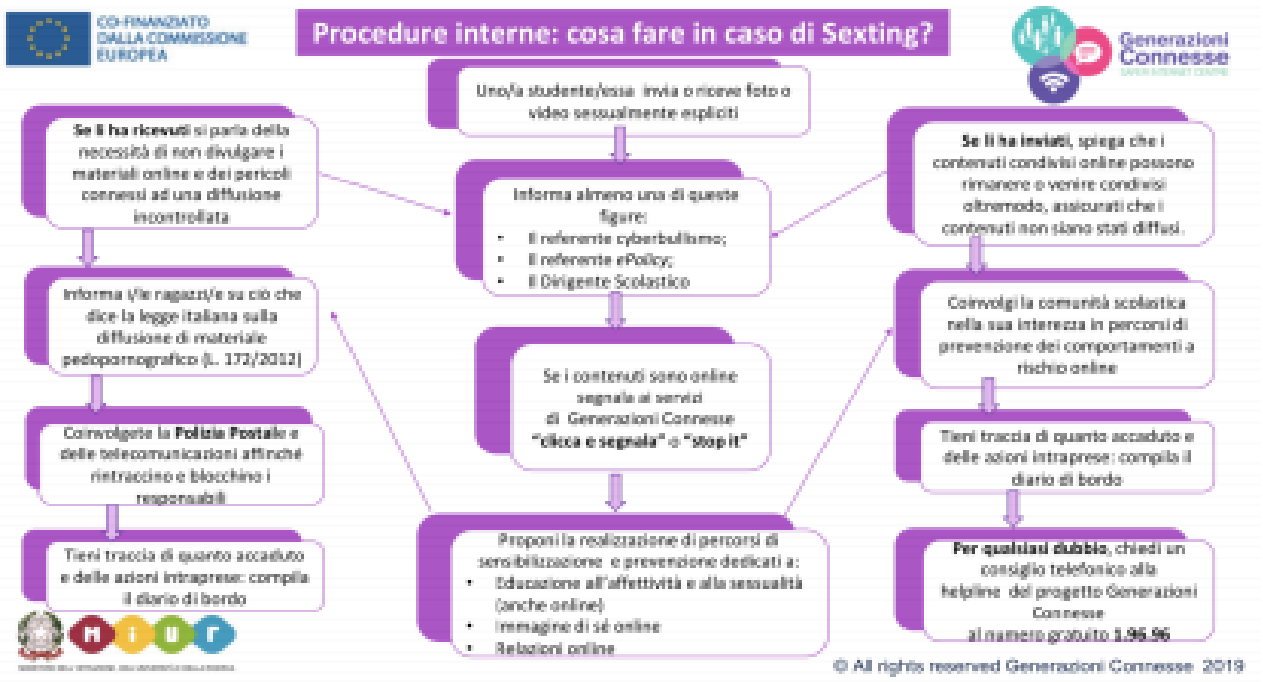
- richiedi la consulenza dello sportello psicologico;
- informa i genitori per condividere informazioni e strategie;
- informa i genitori di ragazzi/e infra quattordicennni;
- valuta se segnalare alla Polizia Postale o ad altri servizi territoriali;
- se hai dubbi, consulta l'helpline di Generazioni Connesse.



PROCEDURE INTERNE: COSA FARE IN CASO DI SEXTING?

1. Il docente viene a conoscenza che uno/a studente/essa invia o riceve foto o video sessualmente espliciti.
2. Avvisa il referente per il cyberbullismo e il Dirigente Scolastico.
3. Se i contenuti sono online segnala ai servizi di Generazioni Connesse "clicca e segnala" o "*stop it*" e parla della necessità di non divulgarli.

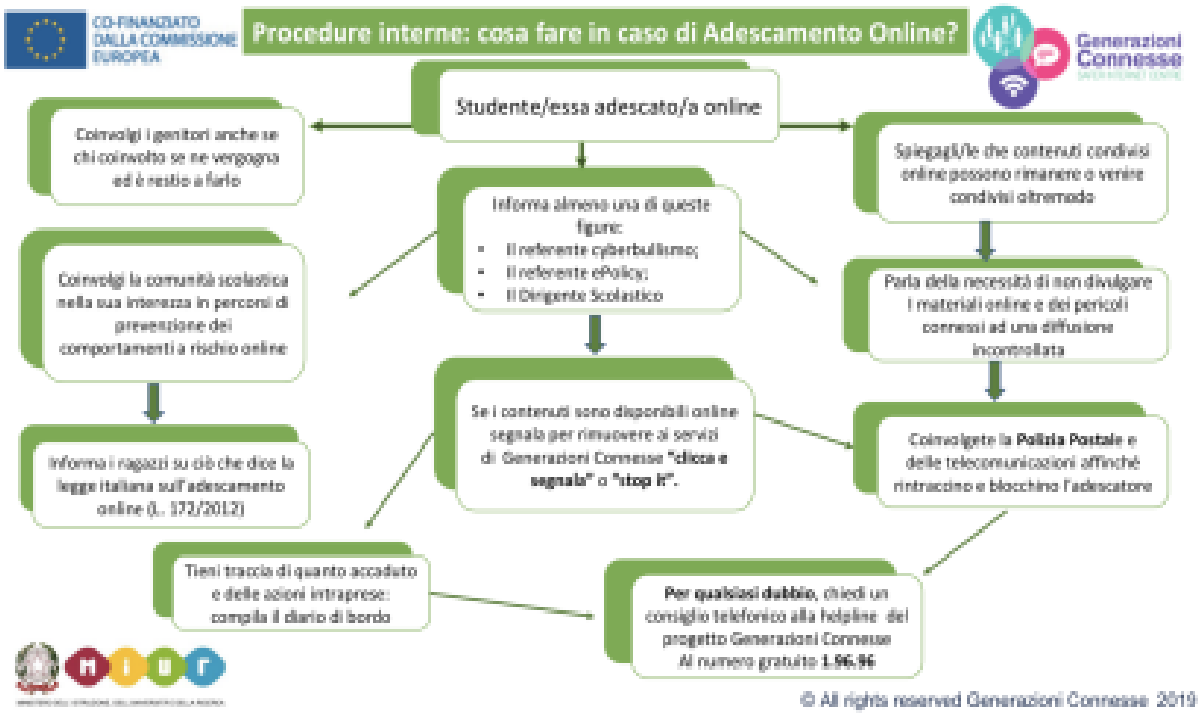
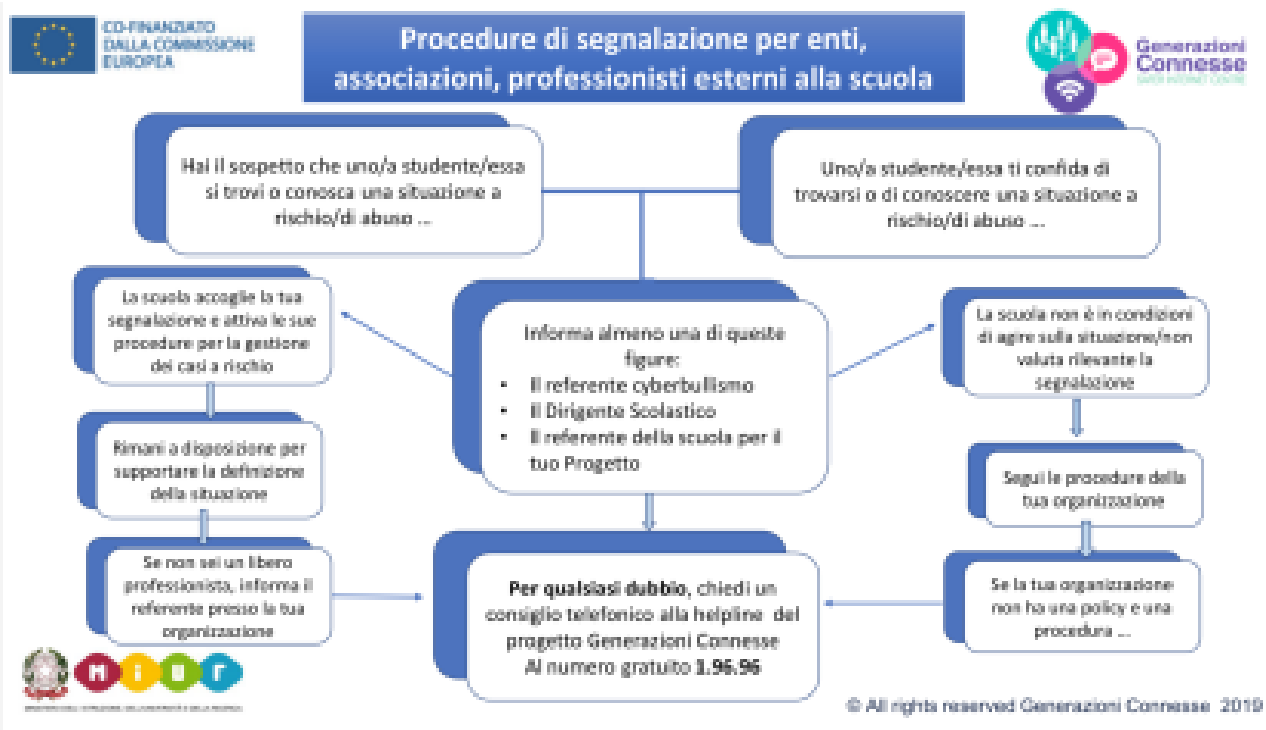
4. Se lo/a studente/essa li ha RICEVUTI, si contatta la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino i responsabili.
5. Informa i/le ragazzi/e su ciò che dice la legge italiana sulla diffusione di materiale pedopornografico (L. 172/2012) e propone percorsi di sensibilizzazione e prevenzione.
6. Tieni traccia dell'accaduto e delle azioni intraprese.
7. Se hai dei dubbi consulta l'helpline di Generazioni Connesse (19696).



PROCEDURE INTERNE: COSA FARE IN CASO DI ADESCAMENTO ONLINE?

1. Il docente viene a conoscenza che uno/a studente/essa è stato/a adescato/a online.
2. Avvisa il referente per il cyberbullismo e il Dirigente Scolastico.
3. Se i contenuti sono online segnala ai servizi di Generazioni Connesse "clicca e segnala" o "stop it" per rimuoverli.
4. Coinvolgi i genitori e la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online.
5. Informa i/le ragazzi/e su ciò che dice la legge italiana sull'adescamento online (L. 172/2012) e spiega che i contenuti condivisi online possono rimanere o venire condivisi e dei pericoli connessi a una diffusione incontrollata.
6. Contatta la Polizia Postale e delle telecomunicazioni affinché rintraccino e blocchino gli adescatori.
7. Tieni traccia dell'accaduto e delle azioni intraprese.

8. Se hai dei dubbi consulta l'helpline di Generazioni Connesse (19696).



PROCEDURE DI SEGNALAZIONE PER ENTI, ASSOCIAZIONI, PROFESSIONISTI ESTERNI ALLA SCUOLA