E-Policy
Istituto Comprensivo di Cembra

Con il supporto del Safer Internet Centre - Ministero dell'Istruzione

1. Presentazione del documento di e-Policy

1.1 Scopo dell'e-Policy

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.

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 le 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

- è responsabile dei dati di alunni e personale della loro sicurezza conosce le procedure da attuare in caso di infrazione della Policy;
- effettua i controlli previsti dalla legge per verificare il corretto utilizzo degli strumenti di lavoro da parte del personale scolastico e degli studenti;
- s'impegna a favorire la sicurezza anche on-line di tutti i membri della comunità scolastica;
- contribuisce, insieme al referente alla prevenzione e contrasto del cyberbullismo all'Animatore Digitale, ad organizzare corsi di formazione specifici per tutte le figure scolastiche sull'uso positivo e responsabile delle TIC;
- accoglie le segnalazioni che i docenti ritengono debbano essere effettuate;
- accoglie le segnalazioni dei casi di presunto cyberbullismo e sovrintende alla loro gestione, in collaborazione con il referente alla prevenzione e

contrasto del Cyberbullismo.

Animatore Digitale e Gruppo di Lavoro TIC

- si occupano della diffusione della Policy fra i colleghi;
- si relazionano con i docenti della scuola, fornendo supporto in caso di difficoltà o dubbi in merito all'attuazione della Policy;
- sono promotori di percorsi di formazione interna all'istituto negli ambiti di sviluppo della scuola digitale, previa rilevazione dei bisogni didattico-formativi dei docenti;
- supportano il personale scolastico anche in riferimento ai rischi online.

Referente alla prevenzione e contrasto del Cyberbullismo

- coordina e promuove tutte le azioni di prevenzione e contrasto del cyberbullismo;
- d'intesa con il Dirigente Scolastico, si avvale della collaborazione delle forze di polizia, delle associazioni e dei centri di aggregazione giovanile del territorio;
- coinvolge studenti, docenti e genitori nella realizzazione di progetti e percorsi formativi;
- d'intesa con il Dirigente Scolastico, accoglie le segnalazioni dei casi di presunto Cyberbullismo e coadiuva il Dirigente nella loro gestione.

Docenti

- diffondono la cultura dell'uso responsabile delle TIC e della Rete, anche integrando parti del curriculum della propria disciplina con approfondimenti ad hoc;
- vigilano attivamente e attentamente gli alunni quando lavorano con le nuove tecnologie e li supportano in caso di difficoltà;
- utilizzano le tecnologie in modo consapevole e professionale, anche quando comunicano con gli studenti;

- utilizzano materiale didattico che rispetti le leggi sui diritti d'autore;
- condividono con il proprio team docenti e/o Consiglio di Classe le situazioni di cui vengono a conoscenza e che considerano rischiose;
- segnalano al Dirigente Scolastico qualunque problematica, violazione o abuso che vede coinvolti studenti e studentesse.

Personale ATA

- collabora nel controllo dell'uso delle tecnologie da parte degli studenti segnalando alla dirigenza, attraverso le procedure contenute nella Policy, le situazioni ritenute rischiose e stabilendo con essa eventuali tempi e modalità di azione.

Tecnico-informatico di Istituto

- su indicazione del Dirigente Scolastico, può accedere a tutti i file dell'area intranet e controllarne i contenuti;
- è l'unico autorizzato all'installazione di nuovi software;
- limita, attraverso un proxy, l'accesso a determinati siti;
- gestisce il firewall presente in ciascun plesso scolastico;
- collabora nella gestione delle prenotazioni dei laboratori informatici, dei laboratori mobili e di ogni altra apparecchiatura informatica.

Studenti e Studentesse

- usano al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti e dalla presente e-Policy,
- online, tutelano e rispettano se stessi e i propri compagni;
- partecipano attivamente a progetti ed attività che riguardano l'uso positivo delle TIC e della Rete;
- conoscono e rispettano i regolamenti scolastici che regolano anche l'attività didattica on-line;

- utilizzano responsabilmente le tecnologie e le immagini, comprendendo che l'utilizzo improprio rappresenta una lesione della privacy altrui e un reato punibile a tutti gli effetti;

- segnalano tempestivamente qualsiasi situazione percepiscano come rischiosa o riconoscano come abuso;

- in ambiente scolastico e/o nel corso di attività didattiche curricolari ed extracurricolari, utilizzano Internet in maniera responsabile, senza cercare o produrre materiale inappropriato o offensivo;

Genitori

- affiancano l'istituto nel promuovere la sicurezza on-line, anche al di fuori del contesto scolastico;

- si relazionano in modo costruttivo con i docenti sulle linee educative che riguardano le TIC e la Rete;

- segnalano usi scorretti della Rete e comunicano con i docenti circa i problemi rilevati quando i propri figli non usano responsabilmente le tecnologie digitali o Internet;

- condividono la visione educativa-formativa e organizzativa prevista dalla Policy d'Istituto.

Enti Educativi esterni e Associazioni del territorio che collaborano con l'Istituto

- si confrontano costruttivamente con la scuola riguardo all'uso consapevole della rete e delle TIC;

- promuovono comportamenti adeguati sulla sicurezza on-line e assicurano la protezione degli studenti e delle studentesse durante le attività che svolgono su mandato della scuola o in partenariato con l'Istituto;

- condividono la visione educativa-formativa e organizzativa prevista dalla Policy d'Istituto.

1.3 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 dell'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. Pertanto i soggetti esterni, prima di avviare la collaborazione educativa richiesta, sono tenuti a prendere visione del presente documento e del PUA (Politica di Uso Accettabile) 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).

1.4 Condivisione e comunicazione dell'e-Policy 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 adottato dal Consiglio dell'Istituzione e viene esposto in versione semplificata negli spazi dell'Istituto che dispongono di pc collegati alla Rete e in tutti i luoghi dell'Istituto ritenuti idonei.

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.

1.5 Gestione delle infrazioni alla e-Policy

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.

Per le infrazioni e relative sanzioni previste dall'istituto si rimanda al Regolamento di Disciplina approvato e pubblicato sul sito della scuola al seguente indirizzo: https://www.iccembra.it/documenti/documenti-istituto/

1.6 Integrazione dell'e-Policy 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 con la specifica normativa nazionale e provinciale.

1.7 Monitoraggio dell'implementazione della e-Policy 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 in Collegio Docenti.

Il monitoraggio della e-Policy è supervisionato dal Dirigente Scolastico che si avvale del Gruppo di lavoro TIC, dell'Animatore Digitale, del referente alla prevenzione e al contrasto del Cyberbullismo, dai referenti TIC di plesso e delle coordinatrici di plesso anche per raccogliere eventuali segnalazioni o comunicazioni ritenute importanti.

Il monitoraggio del documento sarà realizzato a partire da una valutazione della sua efficacia in riferimento agli obiettivi specifici che lo stesso si pone.

2. Formazione e curricolo

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 curricolo digitale.

La scuola, per implementare le competenze digitali degli studenti, adotta le piattaforme didattiche ritenute idonee secondo le modalità specificate nel capitolo 3 del presente documento .

Tenendo conto di Piano Scuola Digitale (PNSD), in particolar modo il paragrafo 4.2. su "Competenze e contenuti", Sillabo sull'Educazione Civica Digitale, DigComp 2.1 e Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente (C189/9, p. 9), considerando il Piano Provinciale Scuola Digitale e il Piano Digitale di Istituto, l'istituto individua cinque aree di competenza da sviluppare e che sono incluse nel curriculum dello studente:

- Area 1: “Alfabetizzazione su informazioni e dati”.
- Area 2: “Comunicazione e collaborazione”.
- Area 3: “Creazione di contenuti digitali”.
- Area 4: “Sicurezza”.
- Area 5: “Risolvere problemi”

Descrittori, livelli di padronanza e modalità valutative sono specificati nel Curricolo Cittadinanza Digitale d’Istituto.

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, anche alla luce dell’introduzione della Didattica Digitale Integrata e della Didattica a Distanza.

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.

Pertanto l’Istituto riconosce e favorisce la partecipazione del personale ad iniziative promosse sia direttamente dalla scuola, dalle reti di scuole e dall’amministrazione, sia quelle liberamente scelte dai docenti (anche online) sulle TIC e si impegna a organizzare ogni anno momenti di formazione sui metodi e sugli strumenti della didattica digitale.

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

La scuola s’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 periodicità,

verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno e del personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio, delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti. La scuola individua come primo strumento di formazione per docenti il sito Generazioni Connesse.

2.4 Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi a 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'e-Policy 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.

Per i genitori degli studenti, la scuola individua, come primo strumento di approfondimento delle tematiche in oggetto, il sito Generazioni Connesse.

2.5 Il nostro piano delle azioni

Da sviluppare entro il termine dell'anno scolastico 2021/2022

- Aggiornare l'attuale Patto di Corresponsabilità;
- Realizzazione di sezione dedicata alla e-Policy sul sito web della scuola;
- Redazione dell'estratto della e-Policy;
- Redazione del documento P.U.A. (Politica di Uso Accettabile);
- Predisposizione di strumento utile per effettuare annualmente un'analisi del

fabbisogno formativo del corpo docente in merito agli obiettivi previsti dal Piano Digitale di Istituto e della Didattica Digitale Integrata;

- Predisposizione di strumento utile per effettuare annualmente un'analisi del fabbisogno formativo-educativo delle famiglie in merito all'uso consapevole e sicuro di Internet e delle Tecnologie digitali.

Da sviluppare entro il termine dell'anno scolastico 2023/2024

- Mettere a regime l'analisi annuale del fabbisogno formativo del corpo docente in merito agli obiettivi previsti dal Piano Digitale di Istituto e della Didattica Digitale Integrata;
- Mettere a regime l'analisi annuale del fabbisogno formativo-educativo delle famiglie in merito all'uso consapevole e sicuro di Internet e delle tecnologie digitali;

- Organizzare almeno due incontri formativi all'anno con enti esterni in merito agli obiettivi previsti dal Piano Digitale di Istituto e della Didattica Digitale Integrata;

- Organizzare almeno due incontri formativi all'anno con enti esterni in merito all'uso consapevole e sicuro di Internet e delle tecnologie digitali;

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". (vedasi: 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.

In questo paragrafo dell'e-Policy 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.

Per visionare tutti di documenti di Istituto in materia di trattamento dei dati personali, tutela della privacy e del diritto alla riservatezza, si rinvia alla sezione del sito web della scuola dedicata alla Privacy: https://www.iccembra.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. 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 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". Tali obiettivi sono condivisi anche dal Piano Provinciale Scuola Digitale e dal Piano Digitale di

Istituto.

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.

La scuola garantisce al personale scolastico e agli studenti il diritto a internet attraverso un'infrastruttura di rete adeguata alle necessità di ciascun plesso e in grado di supportare il traffico dati generato da un numero elevato di utenti. La connessione è in fibra ed è cablata sulla quasi totalità dell'istituto; è infine dotata di firewall gestiti direttamente dal tecnico-informatico all'Istituto.

Interventi periodici di manutenzione e verifica sono programmati dal Dirigente Scolastico in accordo con il tecnico-informatico della scuola. Altre verifiche possono essere compiute su segnalazione dell'Animatore Digitale, dei referenti TIC di plesso e delle coordinatrici di plesso.

La segreteria didattica, quella amministrativa, l'ufficio della RAS e della Dirigente Scolastica sono connesse a rete LAN dedicata e a server indipendente ubicato in un'aula appositamente predisposta all'interno del plesso scolastico della sede centrale.

L'infrastruttura di rete nell'istituto è così organizzata:

<u>Plesso SSPG Cembra:</u>

Rete WIFI = a cui sono connessi tutti i pc delle aule, le LIM, i tablet, i notebook, il laboratorio mobile, l'aula Docenti;

Rete LAN = a cui sono connessi tutti i pc del laboratorio di Informatico;

Rete LAN (intranet)= a cui sono connessi tutti i pc di tutti gli uffici e della Dirigenza Scolastica

Presenza di server condiviso con la SP e di firewall.

<u>Plesso SP Cembra:</u>

Rete WIFI = a cui è connesso il laboratorio mobile;

Rete LAN = a cui sono connessi tutti i pc delle aule, le LIM, tutti i pc del laboratorio di Informatico, l'aula Docenti;

Plesso SSPG Segonzano:

Rete WIFI = a cui sono connessi tutti i pc delle aule, le LIM;

Rete LAN = a cui sono connessi tutti i pc del laboratorio di Informatico, l'ufficio della coordinatrice di plesso, l'aula Docenti;

Presenza di server condiviso con la SP e di firewall.

Plesso SP Segonzano:

Rete WIFI = = a cui sono connessi tutti i pc delle aule e il laboratorio mobile;

Rete LAN = a cui è connessa l'aula Docenti;

Plesso SSPG Giovo:

Rete WIFI = a cui sono connessi tutti i notebook;

Rete LAN = a cui sono connessi tutti i pc del laboratorio di Informatico, tutti i pc delle aule, le LIM; l'ufficio della coordinatrice di plesso, l'aula Docenti;

Presenza di server indipendente (non condiviso con la SP) e di firewall.

Plesso SP Giovo:

Rete WIFI = = a cui è connesso il laboratorio mobile;

Rete LAN = a cui sono connessi tutti i pc delle aule, l'aula Docenti;

Presenza di server indipendente (non condiviso con la SSPG).

Presenza di firewall.

Plesso SP Faver:

Rete WIFI = = a cui è connesso il laboratorio mobile;

Rete LAN = a cui sono connessi tutti i pc delle aule, l'aula Docenti;

Presenza di firewall.

Plesso SP Lases:

Rete WIFI = = a cui sono connessi i notebook;

Rete LAN = a cui sono connessi tutti i pc delle aule, l'aula Docenti, il laboratorio di

Informatica;

Presenza di firewall.

Plesso SP Sover:

Rete WIFI = = a cui sono connessi i notebook;

Rete LAN = a cui sono connessi tutti i pc delle aule, l'aula Docenti, il laboratorio di Informatica;

Presenza di firewall.

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.

Il sito web della scuola è lo strumento utilizzato dall'Istituto sia per raggiungere obiettivi esterni, al fine di valorizzare e promuovere le attività portate avanti dall'Istituto, sia per far circolare all'interno della scuola informazioni di servizio o contenuti importanti fra i diversi attori scolastici

Inoltre l'Istituto utilizza il registro elettronico quale strumento per gestire in modo velocee efficace una comunicazione capillare con tutte le famiglie e con tutto il personale scolastico.

In particolare le famiglie possono, attraverso di esso, visualizzare molte informazioni utili, interagendo con la scuola, su: andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari); risultati scolastici (voti, documenti di valutazione); udienze (prenotazioni colloqui individuali); eventi (agenda eventi); circolari e comunicazione varie (comunicazioni di classe, comunicazioni personali).

L'Istituto esclude l'utilizzo dei social media quale strumento utile per qualsivoglia comunicazione scuola/famiglia.

In ambito prettamente didattico, la scuola attualmente adotta per tutto il personale e gli studenti la Google Suite for education, una piattaforma integrata a marchio Google che consente di comunicare e di gestire contenuti didattico-digitali con grande semplicità e flessibilità. L'utilizzo della Google Suite è ritenuta indispensabile per realizzare le azioni didattiche previste dalla Didattica Digitale Integrata.

Inoltre le apps di Google garantiscono sicurezza e privacy, connessione e interoperabilità, comunicazione facilitata tra docenti e studenti.

Ciascun utente ha accesso a una serie di servizi, tra i quali i principali sono:

Studenti

- una casella di posta personale (con estensione @iccembra.it), con spazio di archiviazione illimitato, attiva solo per il tempo di permanenza nell'Istituto;
- Google Drive (collegato alla casella di posta personale d'istituto), che permette di archiviare e condividere online tutti i tipi di file, senza limiti di spazio;
- Google Classroom (collegato alla casella di posta personale d'istituto), per poter accedere all'ambiente virtuale di classe nel quale lavorare attivamente in modalità sincrona e asincrona con i propri docenti, anche ricevendo materiale integrativo.

Docenti

- una casella di posta personale (con estensione @iccembra.it), con spazio di archiviazione illimitato;
- una casella di posta personale (con estensione @scuole.provincia.tn.it), con spazio di archiviazione illimitato;
- Google Drive (collegato sial alla casella di posta personale d'istituto che a quella provinciale), che permette di archiviare online tutti i tipi di file, senza limiti di spazio;
- Google Classroom (collegato sial alla casella di posta personale d'istituto che a quella provinciale) la seconda app viene utilizzata per poter creare l'ambiente virtuale di classe nel quale lavorare attivamente con i propri studenti, in modalità sincrona e asincrona;

Genitori

- una casella di posta per ciascun nucleo famigliare (con estensione @iccembra.it), con spazio di archiviazione illimitato, attiva solo per il tempo di permanenza nell'Istituto del proprio figlio; le famiglie utilizzano tale indirizzo di posta elettronica per comunicare con la Segreteria Studenti, con

la Segreteria Amministrativa, con il Dirigente Scolastico, con i docenti, con il tecnico-informatico;
- Google Meet (collegato alla casella di posta d'istituto), utilizzato per partecipare alle videoriunioni scuola/famiglia.

Tutti gli utenti sono consapevoli che, dal momento in cui ricevono le credenziali di accesso, tutti i servizi offerti sono per dedicati ad un utilizzo esclusivamente scolastico e didattico.

Le famiglie concedono l'autorizzazione alla creazione dell'account e all'utilizzo della Google suite da parte dei figli compilando apposito form.
Dal momento in cui gli account degli studenti vengono creati e attivati, i genitori sono responsabili della vigilanza sull'utilizzo della casella di posta elettronica e delle app ad essa collegate sia sul dispositivo fisso di casa che sui dispositivi mobili di proprietà degli studenti, avendo sempre cura che le finalità di utilizzo siano esclusivamente didattiche.

Le caselle di posta elettronica degli utenti sono impostate in modo tale da non permettere la registrazione su piattaforme di gioco online e sui social network a uso personale.

I docenti sono tenuti a tenere aggiornati i pc di classe, cancellando con frequenza dati sensibili e documenti superflui e/o archiviando nel proprio Drive personale tutti i file utilizzati. Parimenti gli insegnanti sono tenuti a non salvare sui pc collocati in aree comuni (aula informatica e l'aula Docenti) file personali o contenenti dati personali degli alunni.

Gli aggiornamenti periodici sia del software che del Sistema operativo, così come la manutenzione di tutti i pc e i device, sono gestiti unicamente dal tecnico-informatico di Istituto.

La scuola garantisce formazione adeguata a tutto il personale scolastico sulla gestione dei dispositivi elettronici e sulle regole basilari sulla sicurezza.

3.4 Il nostro piano delle azioni

Da sviluppare entro il termine dell'anno scolastico 2021/2022

- Organizzare corso di formazione sulla gestione dei dispositivi elettronici, della GSuite e dei principali sistemi di archiviazione online;
- Sostituire dispositivi elettronici obsoleti.

Da sviluppare entro il termine dell'anno scolastico 2023/2024

- Completare l'implementazione della rete Wifi di ciascun plesso;
- Completare l'implementazione della dotazione di dispositivi elettronici di ciascun plesso.

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.*

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, partecipazione di un proprio referente per ogni autonomia scolastica; sviluppo delle competenze digitali; 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.

Il referente per le iniziative di prevenzione e contrasto 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;

Il referente infine può svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (Progetto di Istituto, PdM, Rav).

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 ai danni di una persona o di un gruppo.

E' estremamente importante tale fenomeno 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;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network.

Ogni anno scolastico e in particolar modo in caso di effettiva necessità il nostro Istituto intende promuovere attività curricolari e/o extracurricolari attraverso le quali affrontare le problematiche connesse al fenomeno in questione. Inoltre intende fornire al personale della scuola, agli studenti e alle loro famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno stesso.

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.

Ogni anno scolastico e in particolar modo in caso di effettiva necessità il nostro Istituto intende promuovere attività curricolari e/o extracurricolari attraverso le quali affrontare le problematiche connesse al fenomeno in questione. Inoltre intende fornire al personale della scuola, agli studenti e alle loro famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno stesso.

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 mediali 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.

Ogni anno scolastico e in particolar modo in caso di effettiva necessità il nostro Istituto intende promuovere attività curricolari e/o extracurricolari attraverso le quali affrontare le problematiche connesse al fenomeno in questione. Inoltre intende fornire al personale della scuola, agli studenti e alle loro famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno stesso.

4.6 Adescamento online

Il ***grooming*** (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali 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).

Ogni anno scolastico e in particolar modo in caso di effettiva necessità il nostro Istituto intende promuovere attività curricolari e/o extracurricolari attraverso le quali affrontare le problematiche connesse al fenomeno in questione. Inoltre

intende fornire al personale della scuola, agli studenti e alle loro famiglie strumenti finalizzati al riconoscimento e alla prevenzione del fenomeno stesso.

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.

4.8 Il nostro piano delle azioni

Da sviluppare entro il termine dell'anno scolastico 2021/2022

Promuovere la partecipazione di docenti e genitori a momenti formativi finalizzati al riconoscimento e alla prevenzione dei fenomeni analizzati nel presente capitolo;

Da sviluppare entro il termine dell'anno scolastico 2023/2024

Promuovere attività curricolari e/o extracurricolari attraverso le quali affrontare le problematiche connesse ai fenomeni analizzati nel presente 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 la prevenzione e il contrasto del Cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola individua le figure che costituiranno preferibilmente un team preposto alla gestione della segnalazione (gestione interna alla scuola, invio ai soggetti competenti). Nello specifico, presso il nostro Istituto, la gestione delle segnalazioni è affidata alla Dirigente Scolastica e al referente per il contrasto e la prevenzione del Cyberbullismo.

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.

Si suggeriscono, 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.

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 si fa riferimento agli allegati con le procedure.

Segnalazione da parte del docente o del personale scolastico

E' importante che a scuola, in tutti i plessi, sia facilmente reperibile la scheda per la segnalazione del presunto caso di cyberbullismo. (Allegato 1)

La compilazione dalla stessa, da parte del docente o del personale scolastico, è il primo passaggio per una corretta gestione di un eventuale problema. E' altresì possibile comunicare direttamente con il referente al contrasto e alla prevenzione del Cyberbullismo e alla Dirigente Scolastica.

Conservare le prove, è utile per fornire elementi utili a cercare di comprendere l'accaduto. Eventuali testimonianze dirette o indirette, devono comunque essere comunicate al referente al contrasto e alla prevenzione del Cyberbullismo e alla Dirigente Scolastica.

Quando si viene a conoscenza di un problema di cyberbullismo non è opportuno che il singolo intraprenda iniziative personali, come ad esempio interrogare bulli e/o le vittime: occorre rivolgersi al personale di cui sopra che, progettando l'intervento e confrontandosi anche con i docenti di classe, prenderà in carico il problema.

La segnalazione alle autorità competenti può avvenire su iniziativa della famiglia del minore coinvolto o può essere fatta dalla scuola.

Strumenti a disposizione di studenti/esse

Premesso che ciascuno studente può fare riferimento alla propria coordinatrice di classe e/o alla coordinatrice del proprio plesso, 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 coordinato dalla psicologa di Istituto;

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

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.

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.

5.4 Il nostro piano delle azioni

Da sviluppare entro il termine dell'anno scolastico 2020/2021

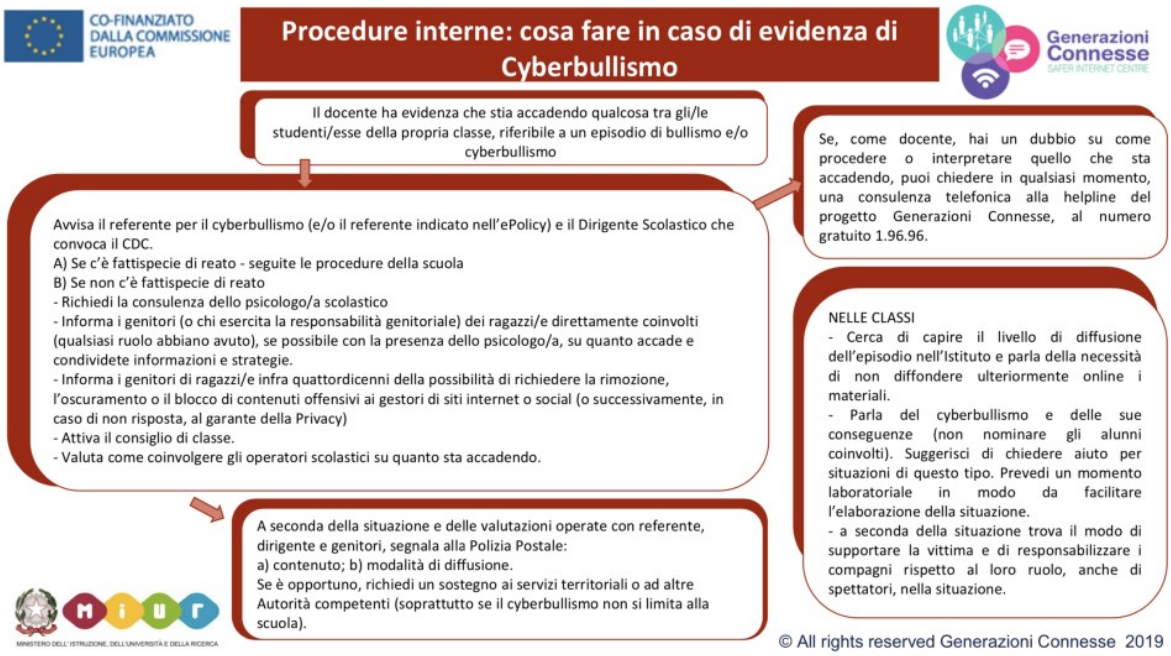
- Attivare un unico indirizzo e-mail di Istituto specifico per le segnalazioni;
- Predisporre in ciascun plesso una scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- Affiggere in ciascuna aula Docenti di ciascun plesso le procedure interne per le segnalazioni di cui al punto successivo.

Da sviluppare entro il termine dell'anno scolastico 2021/2022

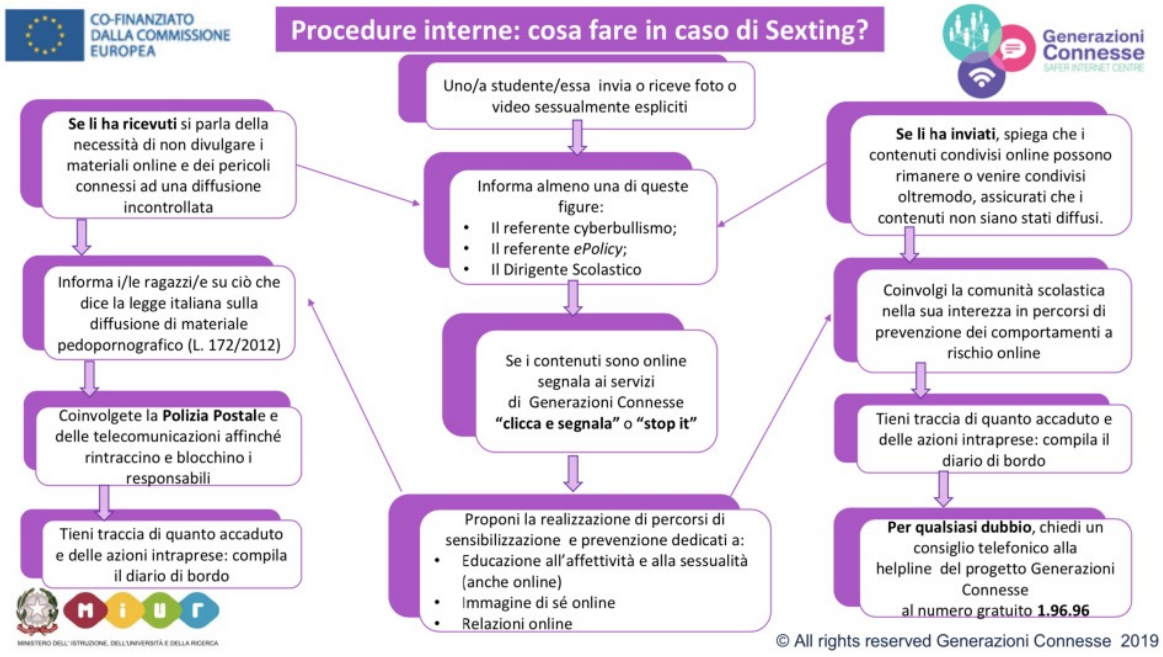
Monitorare efficacia della modalità di segnalazione dei casi sospetti e della loro gestione.

5.5 Allegati con le procedure

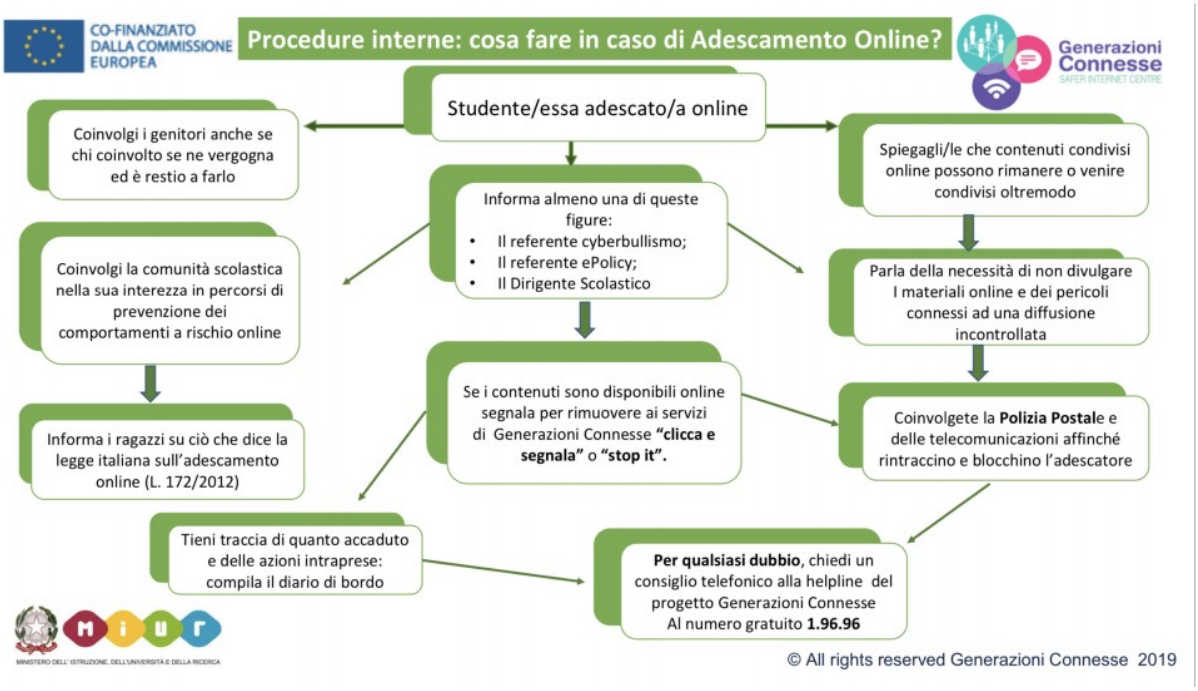
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



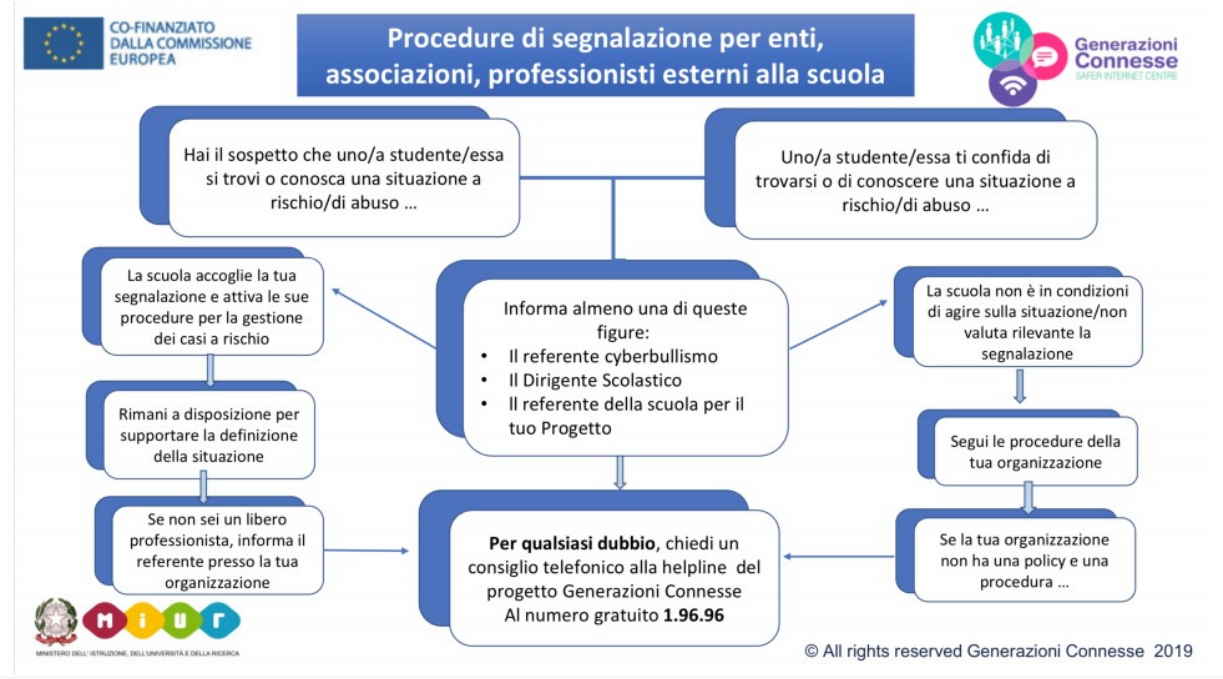
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Scheda di segnalazione interna (Allegato 1)

Scheda di Segnalazione di presunto atto di Cyberbullismo		
Scuola	Primaria/Secondaria di I Grado di……:	
Nominativo e ruolo di chi compila la segnalazione		Docente Personale ATA Genitore Altro _____
Studente coinvolto (presunta vittima): nominativo e classe		
Studente coinvolto (presunto cyberbullo): nominativo e classe		
Eventuali altri studenti coinvolti (presunte altre vittime)		
Eventuali altri studenti coinvolti (presunti altri cyberbulli)		
Date in cui sono accaduti gli episodi da segnalare		
Descrizione degli episodi e dei comportamenti errati che s'intende segnalare		
Elenco eventuali prove telematiche, informatiche o cartacee. Allegare il materiale raccolto		
Data della presente segnalazione		
Firma per accettazione del referente al contrasto e alla prevenzione del Cyberbullismo		