M.I.M. – UFFICIO SCOLASTICO REGIONALE PER L'EMILIA ROMAGNA
ISTITUTO COMPRENSIVO CARPI 3 (MO)
SEDE UFFICI: Via Canalvecchio, 3 - 41012 CARPI (MO)
tel. 059 686618 – Codice Fiscale 90035940361
e Mail: moic83900v@istruzione.it Pec: moic83900v@pec.istruzione.it
Sito web: www.istitutocomprensivocarpi3.edu.it

Documento di e-Policy

(Approvato dal Consiglio di Istituto nella seduta del 07/12/2023)

INDICE

1. Introduzione

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).
Attraverso l'e-Policy l'I.C. Carpi 3 vuole dotarsi di un documento programmatico a cui tutta la comunità educante deve riferirsi, finalizzato a prevenire situazioni problematiche e a riconoscere, gestire, segnalare e monitorare episodi legati ad un utilizzo scorretto degli strumenti, promuovendo nel contempo un uso delle tecnologie positivo e consapevole.
Lo scopo della e-Policy è:
· stabilire i principi fondamentali della comunità scolastica per quanto riguarda l'utilizzo delle tecnologie;
· salvaguardare e proteggere i bambini, i ragazzi e il personale dell'Istituto;
· gestire tramite un protocollo di segnalazione eventuali abusi online, come il cyberbullismo;
· garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che eventuali comportamenti illeciti o pericolosi porteranno a sanzioni disciplinari o addirittura a segnalazioni agli enti competenti.

Le principali aree di rischio per la nostra comunità scolastica riguardano i seguenti ambiti:
contenuto: esposizione a contenuti e siti web non coerenti con le finalità educative d'Istituto, problemi legati all'autenticità e all'esattezza dei contenuti online;
contatto: grooming (adescamento), cyberbullismo in tutte le sue forme, furto di identità;
condotta: privacy (ad es. divulgazione di informazioni personali), reputazione online, diritti e doveri degli internauti (con riferimento alla Cittadinanza Digitale), salute e benessere (quantità di tempo speso online su Internet o giochi), sexting (invio e ricezione di immagini personali intime).

1.2 - Perché è importante dotarsi di una e-Policy?

Attraverso l'e-Policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole,

critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

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

L'e-Policy viene aggiornata periodicamente quando si verificano cambiamenti significativi in riferimento all'uso delle tecnologie digitali all'interno della scuola e/o qualora se ne avverta la necessità.

1.3 - 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.

Definizione dei ruoli:

Il ***Dirigente Scolastico*** è garante della sicurezza, anche online, di tutti i membri della comunità scolastica, della conservazione e gestione dei dati, dell'attuazione di regolamenti e-policy, della loro revisione ed implementazione.

L'***Animatore digitale*** supporta il personale scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali. Promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale". Monitora il corretto uso delle TIC a scuola da parte dei vari soggetti presenti.

Il***Team dell'Innovazione Tecnologica e Digitale*** **(formato da docenti)** coinvolge la comunità scolastica nella partecipazione ad attività e progetti attinenti al curricolo digitale della scuola, pubblica e aggiorna il sito scolastico con contenuti attinenti agli scopi della e-Policy, monitora e rileva le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet, propone idee innovative e sostenibili per favorire la diffusione della cultura digitale.

Il ***Referente bullismo e cyberbullismo*** ha il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo (Legge n. 71/2017).

Il ***Team di gestione emergenze bullismo e cyberbullismo (formato da docenti di primaria e sec. di primo grado)*** ha il compito di prendersi a carico le segnalazioni ricevute da tutti gli operatori della comunità scolastica (alunni e genitori inclusi) attuando le procedure previste dal Protocollo del MIUR.

Il ***Responsabile della e-policy*** è il primo contatto per genitori, studenti/esse, personale scolastico e enti/servizi territoriali per le questioni inerenti la protezione dei minorenni. Coordina le procedure di protezione all'interno della scuola. Si assicura che tutto il personale venga aggiornato sulle nuove procedure o su nuovi compiti e protocolli.

I ***Coordinatori di classe*** raccolgono informazioni e segnalazioni, ne riferiscono al Consiglio di Classe,

monitorano situazioni di rischio.

I ***Docenti*** hanno un ruolo centrale nel diffondere la cultura del benessere e della tutela così come dell'uso responsabile delle TIC e della Rete, promuovendo l'uso delle tecnologie digitali nella didattica e l'educazione positiva; pertanto si informano e si aggiornano costantemente, integrano il curricolo digitale all'interno della progettazione didattica ed educativa, rispettano e fanno rispettare il codice di comportamento, le netiquette e le dadiquette nelle comunicazioni con alunni e genitori, segnalano al DS, secondo le procedure definite all'interno della presente e-policy, preoccupazioni, sospetti, abusi rilevati.

Il ***personale Amministrativo, Tecnico e Ausiliario (ATA)*** è coinvolto nella segnalazione di comportamenti non adeguati e/o episodi di bullismo/cyberbullismo e, insieme ad altre figure, può raccogliere, verificare e valutare le informazioni inerenti possibili casi; il/la DSGA, nei limiti delle risorse finanziarie disponibili, garantisce il funzionamento delle infrastrutture e le condizioni di sicurezza dei dispositivi in dotazione all'istituzione scolastica, affianca il DS nella comunicazione istituzionale con le famiglie degli alunni, il territorio ed i fornitori di servizi.

Gli ***Studenti e le Studentesse***, in relazione al grado di maturità e consapevolezza raggiunta, rispettano i/le propri/e compagni/e, utilizzano al meglio le tecnologie digitali in coerenza con quanto richiesto dai docenti, imparando a tutelarsi anche online, sono informati sui regolamenti scolastici e la e-policy collaborando attivamente a progetti sull'uso positivo delle TIC e facendosi promotori di quanto appreso attraverso possibili percorsi di peer education.

I ***Genitori o chi ne fa la veci,*** in continuità con l'Istituto scolastico, sono partecipi e collaborativi nella promozione di stili di educazione positiva, tenendo fede al patto di corresponsabilità educativa anche per l'uso consapevole e responsabile delle TIC e dei device personali; promuovono e/o sostengono presso gli altri genitori azioni di sensibilizzazione sui temi della sicurezza in rete e della tutela dei minori.

Gli ***Enti educativi esterni e le associazioni*** che entrano in relazione con la scuola si conformano alle scelte della stessa in tema di uso consapevole della Rete e delle TIC, promuovendo comportamenti sicuri, sicurezza online ed assicurando la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme.

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

Tutti gli attori esterni che entrano in relazione educativa con gli studenti e le studentesse e con l'Istituto nel suo complesso sono tenuti a:

- mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati; rispettare il principio di interesse superiore del minore; ascoltare e prendere in seria considerazione le opinioni e i desideri dei minori, soprattutto se preoccupati o allertati per qualcosa;
- conformarsi alla politica dell'Istituto riguardo all'uso consapevole della Rete e delle TIC;
- conoscere e rispettare le regole del nostro Istituto sulle modalità di utilizzo dei propri dispositivi personali (smartphone, tablet, pc, etc.) e di quelli in dotazione alla scuola, evitando un uso improprio o comunque deontologicamente scorretto durante le attività con gli studenti e le studentesse;
- rispettare la privacy, soprattutto dei soggetti minorenni, in termini di fotografie, immagini, video o scambio di contatti personali (numero di telefono, mail, chat, profili di social network).

1.5 - 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 a tutta la 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 di e-Policy è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete o comunque esposto in vari punti spaziali dell'Istituto.

Gli studenti e le studentesse vengono informati sul fatto che sono monitorati e supportati nella navigazione on line.

Quanto ai genitori, si procede invitando i rappresentanti di classe a svolgere, su base volontaria, un percorso mirato di formazione sull'uso positivo delle tecnologie il quale li abiliti al successivo coinvolgimento di altri genitori. Il coordinamento delle azioni indirizzate alle famiglie spetta alla figura del counsellor, al responsabile della e-Policy, al referente per il bullismo e il cyberbullismo.

1.6 - 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. Si tenga conto al riguardo a quanto già previsto dalla Legge n. 71/2017 e dal Regolamento di disciplina per la scuola secondaria di primo grado.
Le potenziali infrazioni a carico degli alunni sono identificabili in:
· uso di social network e blog per pubblicare, condividere o, in genere, postare commenti o giudizi offensivi della dignità altrui;
· condivisione di dati personali;
· connessioni a siti proibiti o comunque non autorizzati;
· pubblicazione di foto o immagini (anche nelle loro modifiche, come stickers e meme) non autorizzate e/o compromettenti.

Le infrazioni alla e-Policy possono essere rilevate dal personale scolastico nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori al personale scolastico.

Gli episodi rilevati sono segnalati alla Dirigenza Scolastica e vengono gestiti dal Team di Gestione

Emergenze Bullismo e Cyberbullismo nel rispetto delle procedure di segnalazione.

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.

Infrazioni degli alunni

Gli interventi educativi previsti per gli alunni sono rapportati alla loro situazione personale e alla loro età. Oltre all'eventuale ricorso a provvedimenti disciplinari, è importante prevedere interventi di ri-definizione delle regole sociali di convivenza con la partecipazione consapevole e attiva degli alunni della classe, di prevenzione e gestione positiva dei conflitti, di moderazione dell'eccessiva competitività, di promozione di rapporti amicali, di gestione delle emozioni.

Infrazioni del personale scolastico

Il Dirigente scolastico può controllare l'utilizzo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a Internet; può controllare la posta elettronica inviata/pervenuta a scuola; può procedere alla cancellazione di materiali inadeguati o non autorizzati presenti nel sistema informatico della scuola, conservandone una copia per eventuali successive investigazioni.

Tutto il personale è tenuto a collaborare con il Dirigente scolastico, fornendo ogni informazione utile per le valutazioni dei casi e per l'avvio di procedimenti che possono avere carattere organizzativo gestionale, disciplinare, amministrativo, penale, a seconda del tipo o della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

In presenza di infrazioni è comunque opportuno valutare se la natura e la gravità di quanto accaduto possa comportare la necessità di denunciare l'episodio (con il coinvolgimento ad es. della Polizia Postale).

1.7 - 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 le indicazioni normative generali sui temi in oggetto.

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. L'Educazione alla Cittadinanza Digitale costituisce, infatti, il terzo nucleo dell'insegnamento trasversale dell'educazione civica, ai sensi dell'art. 5 della legge 20 agosto 2019, n. 92.

Il citato art. 5 esplicita le abilità essenziali da sviluppare nei curricoli di Istituto, con gradualità e tenendo conto dell'età degli studenti.

Sviluppare questa capacità a scuola, con studenti che sono già immersi nel web e che quotidianamente si imbattono nelle tematiche proposte, significa migliorare questo nuovo e così radicato modo di stare nel mondo (ON LIFE). Non è più solo una questione di conoscenza e di utilizzo degli strumenti tecnologici, ma del tipo di approccio agli stessi, un tema piuttosto culturale che tecnologico: per questa ragione, affrontare l'educazione alla cittadinanza digitale non può che essere un impegno professionale che coinvolge tutti i docenti contitolari della classe.

L'I.C. Carpi 3 ha iniziato a elaborare alcuni percorsi educativo.didattici all'interno del proprio curricolo di istituto di educazione civica. Lo step successivo sarà quello di declinare in modo puntuale il suddetto curricolo tenendo presenti le tre dimensioni delle competenze digitali - tecnologica, cognitiva, etica e sociale (Raccomandazioni Europee) - e le cinque aree individuate dal DigComp (Informazione, Comunicazione, Creazione di contenuti, Sicurezza e Problem solving).

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

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

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

Nell'Istituto è presente la figura dell'Animatore Digitale e il Team dell'Innovazione.

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

La scuola si impegna a promuovere percorsi formativi per gli insegnanti sul tema dell'uso consapevole delle tecnologie digitali e della prevenzione dei rischi online. Ciò avverrà tramite specifici momenti di aggiornamento che verranno organizzati dall'Istituto scolastico con la collaborazione del personale specializzato interno (animatore digitale, referente bullismo e cyberbullismo) e se necessario del

personale esterno (professionisti qualificati), con il supporto della rete scolastica del territorio (USR, Osservatori regionali sul bullismo, scuole Polo, etc...), delle amministrazioni comunali, dei servizi socio-educativi e delle associazioni presenti.

Nell'istituto opera un team di docenti per il contrasto al bullismo e al cyberbullismo, ai sensi dell'art. 4, Legge n. 71/2017. E' presente un counsellor, che attua un progetto di Sportello d'Ascolto e svolge un'azione di filtro e di prima presa in carico delle segnalazioni; si reca in osservazione presso le classi segnalate dai docenti o su richiesta di intervento da parte delle famiglie, suggerisce ai docenti intervent educativi appropriati, indirizza le famiglie ai servizi socio-medico-assistenziali del territorio quando necessario.

Infine, insieme al team, svolge azioni sistematiche di monitoraggio dei casi di bullismo e cyberbullismo all'interno dell'Istituto.

Il team si occupa anche di organizzare giornate di sensibilizzazione per gli studenti con la partecipazione di associazioni esterne, di Carabinieri, della Polizia di Stato di Carpi e Polizia Postale di Modena.

2.4 - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

Nella prevenzione dei rischi connessi ad un uso non consapevole delle TIC, così come nella promozione di un loro uso positivo e capace di coglierne le opportunità, è necessaria la collaborazione di tutti gli attori educanti, ognuno secondo i propri ruoli e le proprie responsabilità. Scuola e famiglia devono rinforzare l'alleanza educativa e promuovere percorsi educativi continuativi e condivisi per accompagnare insieme ragazzi/e e bambini/e verso un uso responsabile e arricchente delle tecnologie digitali.

L'Istituto garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese, anche da enti esterni e territoriali, sul tema delle tecnologie digitali, tramite la pubblicazione sul sito della scuola e sul registro elettronico.

Saranno promosse attività seminariali per i genitori, mentre gli organi collegiali attueranno una revisione sistematica dei regolamenti e del patto di corresponsabilità.

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" (Garante della privacy a 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.

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.

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve periodicamente istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.

Il personale scolastico riceve, altresì, la specifica informativa sul trattamento dei propri dati personali.

Nella comunicazione interna ed esterna, la scuola adotta tutte le misure previste al fine di anonimizzare quanto più possibile i dati trattati.

La scuola emana, inoltre, con apposita circolare annuale, l'informativa sulla privacy rivolta alle famiglie.

3.2 - Accesso ad Internet

L'accesso a Internet nell'Istituto è possibile tramite rete LAN o WI-FI ed è protetto da password. La rete interna della sede centrale e dei plessi è protetta da Firewall.
I pc della rete amministrazione sono coperti dall'antivirus.

Norme di accesso:
L'utilizzo di internet da parte del personale scolastico è consentito in tutta la struttura solo ad esclusivo uso didattico e/o di formazione.
Le classi accompagnate ai laboratori multimediali possono accedervi solo ad esclusivo scopo didattico e sotto la responsabilità di un insegnante.
Internet non può essere usato per scopi vietati dalla legislazione vigente;
L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet.

È vietato inserire sui pc connessi in rete programmi contenenti virus e scaricare software non autorizzati da internet.
Prima di installare qualsiasi programma occorre consultare l'animatore digitale per valutarne la compatibilità.

Nei laboratori multimediali le postazioni degli alunni (client) sono dotate di un account alunno col quale effettuare l'accesso. L'account "docente" è accessibile tramite password fornita dall'Animatore digitale ai soli utenti adulti (personale scolastico); l'account "alunno" è impostato con restrizioni di navigazione attraverso filtri specifici.
I docenti hanno piena autonomia nel collegamento ai siti web autorizzati dal firewall.
L'Animatore digitale periodicamente provvede alla manutenzione e all'aggiornamento di tutta l'infrastruttura e dei dispositivi.

Linee guida di buona condotta dell'utente e buone pratiche nell'uso della rete:

- Rispettare la legislazione vigente;
- Tutelare la propria privacy, quella degli altri utenti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui si ha accesso;
- Rispettare la cosiddetta netiquette (regole condivise che disciplinano il rapportarsi tra utenti della rete, siti, forum, mail e di qualsiasi altro tipo di comunicazione);
- Controllare la validità e l'origine delle informazioni a cui si accede o che si ricevono;
- Rispettare i diritti d'autore e i diritti di proprietà intellettuale.

3.3 - Strumenti di comunicazione online

E-mail

Tutto il personale scolastico e tutti gli alunni (dall'infanzia alla secondaria di primo grado) possono utilizzare i servizi mail accedendo alla rete della scuola a fini esclusivamente didattici e possiedono un account con estensione @carpi3.istruzioneer.it. La nostra scuola, infatti, ha adottato i servizi Google Workspace for Education e gestisce un proprio spazio. L'account è strettamente personale, per cui ogni utente dovrà avere cura di disconnettere il proprio accesso al termine del suo utilizzo. Lo spazio è destinato alla ricezione di comunicazioni, all'invio di documentazione, alla condivisione di materiali e progetti didattici. Sulla rete scolastica tutti sono invitati a utilizzare solo account di posta elettronica presenti nel dominio scolastico e per scopi inerenti lo svolgimento didattico/organizzativo. Le comunicazioni tra personale scolastico, famiglie e allieve/allievi via e-mail devono avvenire preferibilmente tramite un indirizzo e-mail della scuola o all'interno della piattaforma di apprendimento Google Workspace for Education con estensione istituzionale o tramite **registro elettronico**, per consentire l'attivazione di protocolli di controllo. E mail in arrivo da mittenti sconosciuti vanno trattate come sospette ed eventuali allegati non devono essere aperti.

L'account di posta elettronica istituzionale, utilizzato ordinariamente dagli uffici amministrativi e dagli utenti esterni oltre che dal personale scolastico, è moic83900v@istruzione.it.

Sito web della scuola

Il Dirigente Scolastico e il personale incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato ed appropriato. La scuola offre all'interno del proprio sito una serie di servizi alle famiglie e ai fruitori esterni; i docenti che desiderano pubblicare attività didattiche dovranno chiedere l'autorizzazione al Dirigente. Il provider fornitore dei servizi di segreteria digitale, registro elettronico, sito web e gestione del personale, è il Gruppo Nuvola Madisoft che gestisce l'archiviazione e la storicizzazione di tutti i dati trattati ai fini istituzionali.

La scuola ha di recente rinnovato ed adeguato alla luce della normativa vigente, il sito web istituzionale https://www.istitutocomprensivocarpi3.edu.it/

Tutti i contenuti sono pubblicati sotto la diretta supervisione ed autorizzazione del Dirigente scolastico che ne garantisce la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy.

L'Associazione D.A.G.A.H. (Docenti, Alunni, Genitori, Ata, Hack) gestisce autonomamente un sito web http://www.dagah.it, dove condivide e rende pubbliche le principali iniziative scolastiche, gli eventi, le premiazioni e tutto ciò che connota in senso positivo la vita della Scuola Secondaria di primo Grado "M. Hack".

Registro elettronico

Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente è tenuto a registrare assenze, valutazioni, note e osservazioni. Le famiglie, attraverso di esso, possono visualizzare molte informazioni utili, interagendo con la scuola su: andamento scolastico (assenze, argomenti delle lezioni e compiti, note disciplinari); risultati scolastici (voti, documenti di valutazione); udienze (prenotazioni di colloqui individuali); eventi (agenda eventi); comunicazioni varie (circolari, comunicazioni di classe, comunicazioni personali).

Coloro che non possono accedere a Internet e di conseguenza non possono consultare il registro elettronico devono darne segnalazione all'ufficio di segreteria.

Per l'utilizzo del registro elettronico dell'I.C. Carpi 3 si fa riferimento alla modalità di utilizzo della piattaforma Nuvola Madisoft, erogatrice dei servizi didattici dell'Istituto.

3.4 - Strumentazione personale

La presente e-Policy contiene indicazioni, revisioni o eventuali integrazioni dei Regolamenti interni già esistenti che disciplinano l'uso dei dispositivi personali in classe.

Come previsto dalla normativa vigente e dal Regolamento d'Istituto, è fatto divieto a chiunque di utilizzare il telefono cellulare durante le ore di lezione.

La violazione di tale divieto configura un'infrazione disciplinare rispetto alla quale la scuola è tenuta ad applicare apposite sanzioni.

Nel caso debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare gratuitamente la linea fissa della scuola rivolgendosi ad un collaboratore scolastico; allo stesso modo le famiglie sono tenute a chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

Gli alunni potranno usare i propri dispositivi informatici quali smartphone, tablet o notebook nelle ore di lezione solo se autorizzati dai docenti e solo per motivi didattici.

Resta il divieto di fare foto o video se non autorizzati.

Ai sensi della stessa Direttiva Ministeriale, con la condivisione della presente e-Policy, "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone". L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati, così come, in base al DM n. 104 del 30/11/2007 "Linee di indirizzo e chiarimenti sulla normativa vigente sull'uso di telefoni cellulari e di altri dispositivi elettronici nelle comunità scolastiche" è punibile civilmente e penalmente chi abusa dei dati personali altrui raccolti (immagini, filmati, registrazioni vocali…) violandone la privacy.

Riguardo all'uso scorretto dello smartphone, si ricorda in particolare che:

- la scuola non pone alcun ostacolo all'utilizzo di hard - disk portatili come strumenti di lavoro e di studio. Compete alle famiglie il controllo del contenuto di questi strumenti per evitare che qualche

studente 'trasporti' a scuola immagini, testi o filmati 'sconvenienti', magari scaricati solo per curiosità;

- fermo restando che la scuola è un'istituzione educativa e che non è possibile né tantomeno legittima la perquisizione quotidiana degli studenti all'inizio di ogni giorno di lezione, le responsabilità che dovessero derivare dal verificarsi di eventi riconducibili all'uso non corretto o non legittimo di uno qualsiasi degli oggetti di cui alla presente norma regolamentare sono tutte ascrivibili alle famiglie degli studenti eventualmente coinvolti;
- le responsabilità sopra menzionate sono condivise dal personale scolastico solo se esso, avendo personalmente constatato o essendo venuto a conoscenza di un uso improprio di un device (smartphone o tablet) da parte di un ragazzo/a durante l'orario scolastico, non dovesse immediatamente intervenire per impedire tale comportamento.

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 conoscere i rischi legati ad un utilizzo non consapevole del digitale e della Rete e saperli distinguere tra loro in modo da poter poi adottare le strategie migliori per poterli arginare e contenere, ma è altrettanto importante adottare degli interventi di sensibilizzazione e prevenzione per poter ridurre l'incidenza di situazioni di rischio.

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.*

L'I.C. Carpi 3 s'impegna a: accrescere la consapevolezza circa il fenomeno del bullismo e del cyberbullismo; incoraggiare i soggetti più fragili a modificare i propri comportamenti rendendoli più funzionali; promuovere il benessere personale, il clima positivo del gruppo classe, la sicurezza nella scuola; favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva.

Nel caso della **prevenzione** *si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali allo scopo di evitare l'insorgenza di rischi legati ad un uso improprio delle stesse.*

L'I.C. Carpi 3 s'impegna a: monitorare costantemente le relazioni interne alla classe, onde individuare possibili situazioni di disagio ed intervenire tempestivamente; indirizzare il gruppo verso l'instaurazione di un clima positivo di reciproca accettazione e rispetto; integrare nel curricolo temi legati al corretto utilizzo delle TIC e di Internet; supportare e implementare la competenza digitale in tutti i ragazzi all'interno delle materie curricolari.

L'I.C. Carpi 3 ha scelto una politica interna che sia pro-attiva, tesa cioè a creare un ambiente di apprendimento sereno e sicuro, in cui non sono permessi cyberbullismo, prepotenza, aggressione e violenza.

Azioni

È buona prassi che tutto il personale scolastico, le famiglie e gli alunni sappiano che è possibile chiedere aiuto o informazioni 24h su 24 attraverso il telefono, la chat, l'email e navigando su siti internet sicuri e garantiti come Generazioni Connesse (www.generazioniconnesse.it). Oltre agli adulti di riferimento (quali la famiglia, gli insegnanti e/o altri educatori che rivestono un ruolo significativo nella vita del minore) esistono altre modalità e strumenti per chiedere informazioni, supporto e aiuto, tra cui:

- due servizi messi a disposizione dal Safer Internet Center italiano: sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children. Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia.
- 1.96.96: numero per l'helpline e la chat del Telefono Azzurro: essa accoglie qualsiasi richiesta di ascolto e di aiuto da parte di bambini/e e ragazzi/e fino ai 18 anni o di adulti che intendono confrontarsi su situazioni di disagio/pericolo in cui si trova un minorenne. Il servizio è riservato, gratuito e sicuro, dedicato ai giovani o ai loro familiari che possono chattare, inviare e-mail o parlare al telefono con professionisti qualificati relativamente a dubbi, domande o problemi legati all'uso delle nuove tecnologie digitali e alla sicurezza online. Fornisce il supporto per la hotline (ovvero la denuncia e il contrasto del fenomeno) e l'helpline (per la gestione e la presa in carico dello stesso).
- 114: Emergenza Infanzia: è un modello multiagency che, oltre all'utente coinvolto, può attivare anche le Forze dell'Ordine, i Servizi Sociali, le agenzie del territorio, le procure, il MIM.
- 116.000: Numero Unico Europeo per minori scomparsi, o minori stranieri non accompagnati.

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".

Il cyberbullismo è la manifestazione in rete del fenomeno del bullismo perpetrato in modo continuo, ripetuto e sistematico soprattutto attraverso i social network, con la diffusione di messaggi offensivi, foto, video e immagini denigratorie o tramite la creazione di gruppi contro. Si tratta di un fenomeno molto grave perché in pochissimo tempo le vittime possono vedere la propria reputazione danneggiata in una comunità molto ampia, anche perché i contenuti, una volta pubblicati, possono riapparire a più riprese in luoghi diversi.

E' possibile suddividere gli atti di cyberbullismo in due grandi gruppi:

- cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei;
- cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

I tratti specifici del bullismo online sono correlati all'impatto che le tecnologie digitali hanno nella vita dei ragazzi e alle caratteristiche stesse della Rete:

- L'impatto: la diffusione incontrollabile dei contenuti immessi in rete;

- La convinzione dell'anonimato: "falso mito della Rete", ogni nostra azione online è, infatti, rintracciabile ma rappresenta un fattore del forte stress percepito dalla vittima;

- L'assenza di confini spaziali: spegnere il cellulare o il computer non basta, così come cancellare tutti i propri profili social;

- L'assenza di limiti temporali: può avvenire ad ogni ora del giorno e della notte;

- L'indebolimento dell'empatia: online la funzione speciale dei neuroni specchio viene meno e la riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli;

- Il feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni della vittima e ciò riduce fortemente l'empatia e il riconoscimento del danno provocato. La mediazione tecnologica, infatti, porta ad un certo distanziamento fra aggressore e vittima.

A tutto ciò si aggiungono altre convinzioni o tendenze frequenti nell'uso della Rete sia da parte dei giovani che degli adulti:

- Percezione che online non ci siano norme sociali da rispettare;
- La sperimentazione online di identità e personalità multiple;
- Il contesto virtuale come un luogo di simulazione e giochi di ruolo;
- Diffusione di responsabilità: tutti quelli che partecipano anche solo con un like o un commento diventano, di fatto, corresponsabili ma d'altro canto sono proprio loro che possono "fare la differenza".

Chi compie atti di bullismo e cyberbullismo può anche essere responsabile di reati penali e danni civili.

L'I.C Carpi 3 in ottemperanza alla Legge 71/2017 e alle Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo emanate dal MIUR, che indicano al mondo scolastico ruoli, responsabilità e azioni utili a prevenire e gestire i casi di cyberbullismo, si impegna a:
- formare il personale scolastico;
- sviluppare le competenze digitali tra gli obiettivi formativi prioritari (L.107/2015);
- promuovere un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- prevedere misure di sostegno e rieducazione dei minori coinvolti;
- integrare i regolamenti e il patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- attivare un sistema di segnalazione nella scuola;
- valutazione degli studenti a rischio, osservazione del disagio, rilevazione dei comportamenti dannosi per la salute di ragazzi/e;
- prevedere azioni preventive ed educative e non solo sanzionatorie;
- nominare un Referente per le iniziative di prevenzione e contrasto del cyberbullismo, che potrà avvalersi della collaborazione delle Forze di polizia e delle associazioni e centri di aggregazione giovanile del territorio e potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav);
- individuare un team di docenti, appartenenti sia alla scuola primaria che secondaria di primo grado, che opera per il contrasto del fenomeno del bullismo e del cyberbullismo in sinergia con il Dirigente Scolastico.

Inoltre, nella scuola secondaria di primo grado è attivo uno Sportello d'ascolto condotto da un counsellor, che è di fondamentale importanza per gestire e monitorare i casi di bullismo e cyberbullismo segnalati alla scuola.

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

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed è estremamente importante affrontarlo anche a livello educativo e scolastico.

Le azioni di sensibilizzazione (es. giornate a tema, come la Giornata della Gentilezza) e di prevenzione in merito al fenomeno dei "discorsi d'odio" non possono che essere di ampio raggio attraverso il lento e paziente lavoro di interlocuzione con gli studenti, di promozione del pensiero critico e eterocentrato, di scavo ed emersione dei vissuti di rabbia, intolleranza, esclusione, paura. Le attività di natura trasversale, da calare anche nella progettazione di educazione civica, possono tenere conto di alcuni temi sensibili quali:
- la gestione delle emozioni (proprie e altrui) e l'accettazione della diversità;
- come nasce il pregiudizio;
- discriminazione e razzismo nelle società attuali;
- libertà di opinione e di espressione: misura e limiti;
- solidarietà e impegno sociale

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.

L'abuso di gioco virtuale può assumere forme di Dipendenza dal gioco online: ritiro sociale, irritabilità, depressione, pensieri ossessivi sono alcuni dei rischi di questa forma di abuso.

Nella scuola, può essere fondamentale coinvolgere i genitori degli alunni più piccoli nel condividere modelli di genitorialità positiva e nel costituire gruppi di mutuo suorto.

4.5 - Sexting

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

Spesso sono realizzate con il telefonino, e vengono diffuse attraverso il cellulare (tramite invio di mms o condivisione tramite bluetooth) o attraverso siti, e-mail, chat. Tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile. L'invio di foto che ritraggono minorenni

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

I contenuti sessualmente espliciti possono diventare materiale di ricatto assumendo la forma di "revenge porn", letteralmente "vendetta porno", fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge 19 luglio 2019 n. 69, all'articolo 10 ha introdotto in Italia il reato di revenge porn).

Il materiale pubblicato online può permanervi per un tempo illimitato e potrebbe non essere mai definitivamente rimosso. Un contenuto ricevuto, infatti, può essere salvato, a sua volta re-inoltrato oppure condiviso su piattaforme diverse da quelle originarie e/o in momenti successivi.

I rischi del sexting, legati al revenge porn, possono contemplare: violenza psicosessuale, umiliazione, bullismo, cyberbullismo, molestie, stress emotivo che si riversa anche sul corpo insieme ad ansia diffusa, sfiducia nell'altro/i e depressione.

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 rivolgersi alla Polizia Postale, con l'obiettivo di ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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.). 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.

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli segnali che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore;

Il processo di adescamento segue generalmente 5 fasi:
1. **Fase dell'amicizia iniziale**: Questa è la fase in cui l'adescatore cerca i primi contatti con la vittima individuata, provando a socializzare con lei.
2. **Fase di risk-assessment:** in seguito ai primi contatti con il minore, l'adescatore cerca di comprendere il contesto in cui si svolge l'interazione (es. da dove si collega alla Rete? I genitori lo controllano quando chatta? Che rapporto ha con loro?).
3. **Fase della costruzione del rapporto di fiducia**: le confidenze e le tematiche affrontate divengono via

via più private ed intime o comunque molto personali. In questa fase l'adescatore può iniziare a fare regali di vario tipo alla vittima e può anche avvenire lo scambio di foto, subito e non necessariamente a sfondo sessuale.

4. **Fase dell'esclusività**: l'adescatore rende la relazione con il minore sempre più "segreta", isolandolo sempre più dalla famiglia e dagli amici. Chiederà alla vittima di non raccontare a nessuno ciò che sta vivendo.

5. **Fase della relazione sessualizzata**: in questa fase la richiesta di immagini o video sempre più privati e a sfondo erotico potrebbe essere più insistente, così come la proposta di incontri offline.

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

Fondamentale, quindi, è portare avanti un percorso di educazione digitale che comprenda lo sviluppo anche di capacità quali la protezione della propria privacy e la gestione dell'immagine e dell'identità online, la capacità di gestire adeguatamente le proprie relazioni online (a partire dalla consapevolezza della peculiarità del mezzo/schermo che permette a chiunque di potersi presentare molto diversamente da come realmente è).

Se si sospetta o si ha la certezza di un caso di adescamento online è importante, innanzitutto, che l'adulto di riferimento non si sostituisca al minore nel rispondere, ad esempio, all'adescatore. È importante che il computer o altri dispositivi elettronici del minore vittima non vengano usati per non compromettere eventuali prove.

Casi di adescamento online richiedono l'intervento della Polizia Postale a cui bisogna rivolgersi il prima possibile, tenendo traccia degli scambi fra il minore e l'adescatore (ad esempio, salvando le conversazioni attraverso screenshot, memorizzando eventuali immagini o video…).

L'adescamento può essere una problematica molto delicata da gestire e può avere ripercussioni significative sul minore, che deve quindi ricevere un adeguato sostegno psicologico da parte di esperti.

I minori vittime di adescamento riferiscono, generalmente, di sentirsi traditi, ma anche di provare un senso di colpa per essere caduti in trappola ed essersi fidati di uno sconosciuto.

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.

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.

5. Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

Nelle procedure sono indicate:

- le **figure preposte all'accoglienza della segnalazione e alla presa in carico e gestione del caso**;

- le modalità di coinvolgimento del referente per il contrasto del bullismo e del cyberbullismo, oltre al Dirigente Scolastico.

Inoltre, la scuola ha **individuato le figure che costituiscono 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.

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 fare riferimento agli allegati con le procedure che si trovano a fine documento.

Strumenti a disposizione di studenti/esse

I nostri studenti/esse posso segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni a chiunque operi nella scuola. Se si tratta di (cyber)bullismo sarà lo stesso interlocutore a compilare una "scheda di prima segnalazione" prevista dal protocollo MIUR. Per altre situazioni, negli incontri di formazione sui rischi della rete è bene ricordare che anche gli studenti/studentesse possono rivolgersi alle Helpline menzionate precedentemente. Inoltre, è sempre possibile richiedere lo sportello di ascolto con il Counsellor della scuola.

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.

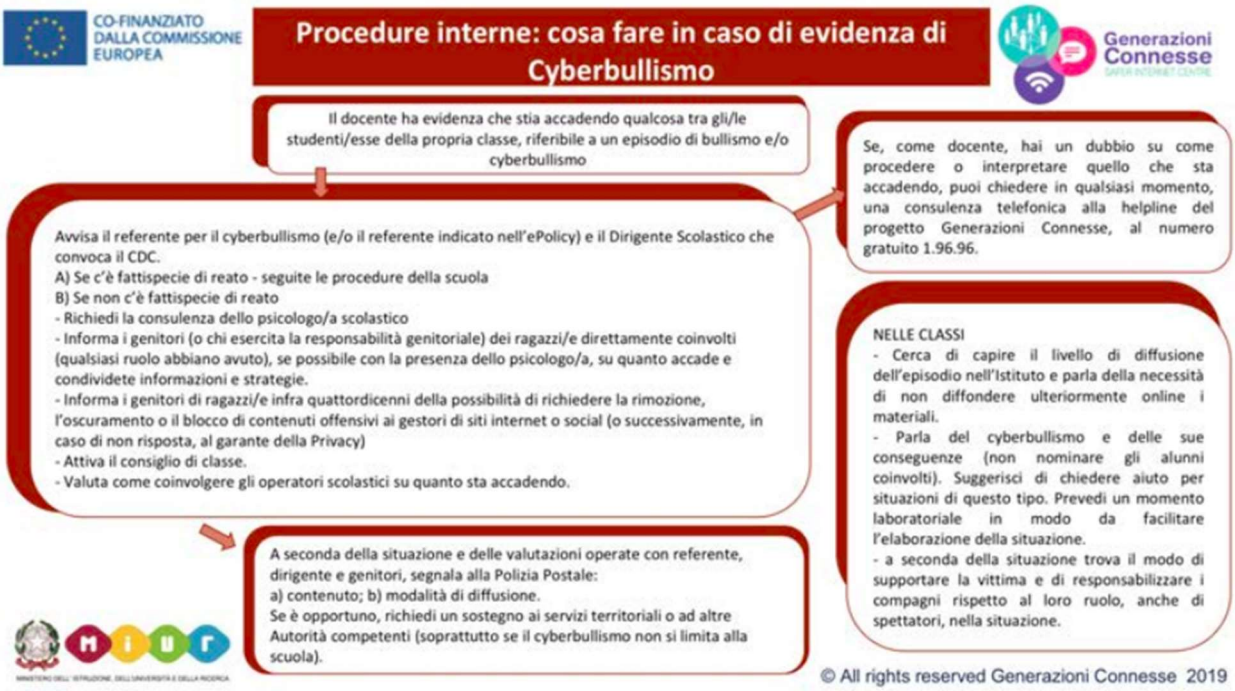
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.
Comitato Regionale Unicef: presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia. E' a Modena (https://www.unicef.it/comitati-locali/modena/)

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 (https://www.assemblea.emr.it/corecom)
Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet (https://www.istruzioneer.gov.it/)
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 (https://www.comune.modena.it/amministrazione/uffici/uffici-di-altri-enti/polizia-postale-e-delle-comunicazioni)

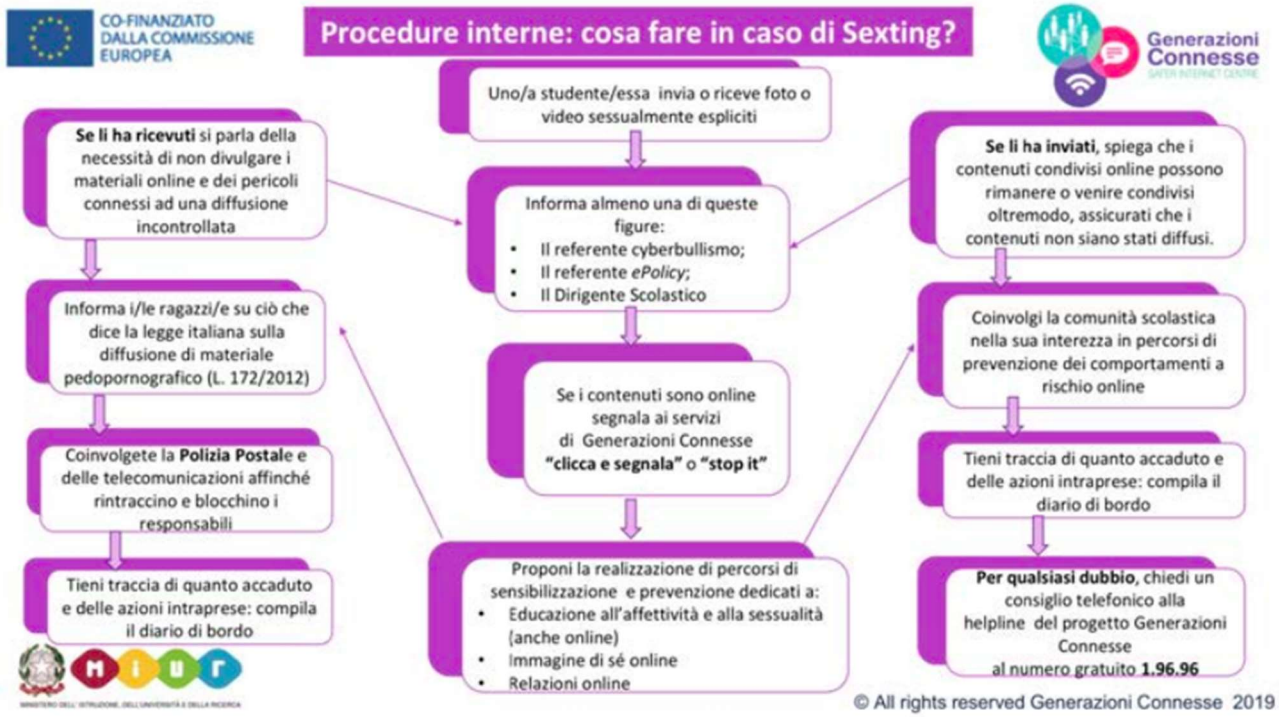
Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di 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 dovuti a situazioni ambientali carenti o inadeguate. (https://www.assemblea.emr.it/garante-minori)
Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

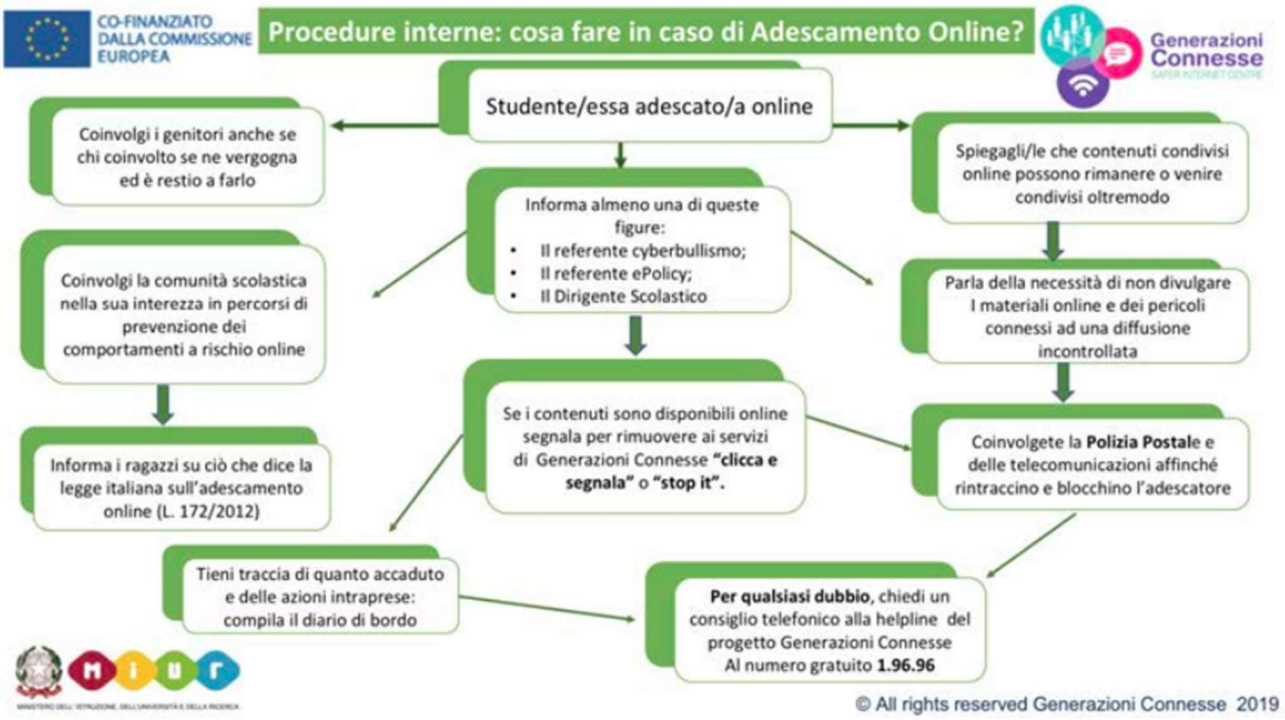
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



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