Scuola Secondaria di I Grado
"Gisella Floreanini"
DOMODOSSOLA (VB)

Via Terracini 23 - 0324/243125
Via Matilde Ceretti 17 -
0324/243649
28845 DOMODOSSOLA (VB)
Cod. Fisc. 83001790035
e-mail: vbmm01700a@istruzione.it
vbmm01700a@pec.istruzione.it

Dirigente scolastico: dott.ssa Chiara Varesi

E-SAFETY POLICY

in pillole

Animatore digitale:
prof.ssa Giada Zerboni
(zerboni.giada@smsdomodossola.it)
Referente cyberbullismo:
prof.ssa Stefania Cerri
(cerri.stefania@smsdomodossola.it)

Generazioni Connesse
SAFER INTERNET CENTRE

SCOPO DELLA *E-SAFETY POLICY*

L' *e-Policy* è 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* 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* viene condivisa e comunicata al personale, agli studenti e alle studentesse, alla comunità scolastica attraverso:
- Pubblicazione del documento sul sito istituzionale della scuola;
- Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico.

Il documento è approvato dal Collegio dei Docenti e dal Consiglio di Istituto e viene esposto in versione semplificata negli spazi che dispongono di pc collegati alla Rete.

INDICE

Nel seguente documento, che è una sintesi di quello integrale inserito nell'area «trasparenza» del sito, si trovano:

RUOLI E RESPONSABILITÀ DI TUTTI I MEMBRI DELLA COMUNITA' SCOLASTICA

DIRIGENTE SCOLASTICO

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

ANIMATORE DIGITALE

- ✓ Stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale";
- ✓ Fornire consulenza e informazioni al personale rispetto ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- ✓ Monitorare e rilevare le problematiche emergenti, relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione, con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- ✓ Assicurare che gli utenti possano accedere alla rete della scuola solo tramite password personali, applicate e regolarmente cambiate, e curare la manutenzione e lo sviluppo del sito web della scuola per scopi istituzionali e consentiti (istruzione e formazione);
- ✓ Coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".

REFERENTE CYBERBULLISMO

- ✓ Supportare il Dirigente scolastico nella revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav);
- ✓ Coordinare le iniziative di prevenzione e contrasto al cyberbullismo. A tal fine, potrà avvalersi della collaborazione delle Forze dell'ordine e delle Associazioni del territorio;
- ✓ Assicurare che l'educazione alla sicurezza online sia incorporata in tutto il programma di studi;
- ✓ Promuovere la consapevolezza e l'impegno per la salvaguardia online in tutta la comunità scolastica;
- ✓ Promuovere la formazione e dare consulenza a tutto il personale;
- ✓ Promuovere attività o progetti da svolgere nelle classi;
- ✓ Applicare e controllare i protocolli di rilevazione, monitoraggio e gestione delle potenziali azioni di cyber bullismo;
- ✓ Diffondere la E- Safety Policy attraverso power point e schede semplificative;
- ✓ Collaborare con tutte le agenzie educative e istituzionali (Associazioni, Polizia postale, Forze dell'ordine, etc.) per prevenire e gestire i casi di possibile cyber bullismo;
- ✓ Coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti l'utilizzo consapevole di internet.

RUOLI E RESPONSABILITÀ DI TUTTI I MEMBRI DELLA COMUNITA' SCOLASTICA

DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

- ✓ assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni;
- ✓ garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.), all'interno della scuola e fra la scuola e le famiglie, per la notifica di documenti e informazioni del dirigente scolastico e dell'animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

PERSONALE SCOLASTICO (Ata, etc.)

- ✓ essere consapevoli dei problemi di sicurezza on-line connessi con l'uso di telefoni cellulari, fotocamere e dispositivi portatili;
- ✓ comprendere e contribuire a promuovere politiche di sicurezza;
- ✓ monitorare l'uso di dispositivi tecnologici e attuare politiche scolastiche per quanto riguarda questi dispositivi;
- ✓ segnalare qualsiasi abuso, anche sospetto, o problema al Dirigente e ai responsabili della sicurezza online;
- ✓ usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia;
- ✓ aver letto, compreso e sottoscritto la presente policy.

DOCENTI

- ✓ informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- ✓ garantire che le modalità di utilizzo corretto e sicuro delle TIC e di internet siano integrate nel curriculum di studio e nelle attività didattiche ed educative delle classi;
- ✓ garantire che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
- ✓ assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete ma anche della necessità di evitare il plagio e di rispettare la normativa sui diritti d'autore;
- ✓ garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali;

RUOLI E RESPONSABILITÀ DI TUTTI I MEMBRI DELLA COMUNITA' SCOLASTICA

DOCENTI

- ✓ Assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- ✓ Controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
- ✓ Nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
- ✓ Comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;

ALUNNI

- ✓ Essere responsabili, in relazione al proprio grado di maturità e di apprendimento, nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- ✓ Avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali e avere consapevolezza della necessità di evitare il plagio e rispettare i diritti d'autore;
- ✓ Comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali;
- ✓ Adottare condotte rispettose degli altri anche quando si comunica in rete;
- ✓ Esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

GENITORI

- ✓ Sostenere la linea di condotta della Scuola, adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- ✓ Seguire gli alunni nello studio a casa, adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti; in particolare, controllare l'utilizzo del pc e di internet;
- ✓ Concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;
- ✓ Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e dello smartphone in generale.
- ✓ Aver letto, compreso e sottoscritto la presente policy.

RUOLI E RESPONSABILITÀ DI TUTTI I MEMBRI DELLA COMUNITA' SCOLASTICA

DOCENTI

- ✓ Segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo, ovvero esigenza di carattere informativo, all'animatore digitale, ai fini della ricerca di soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e ai fini di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- ✓ Segnalare al dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme;
- ✓ Aver letto, compreso e sottoscritto la presente policy.

ENTI EDUCATIVI ESTERNI E ASSOCIAZIONI

- ✓ Conformarsi alla politica della Scuola riguardo all'uso consapevole della Rete e delle TIC;
- ✓ Promuovere comportamenti sicuri e la sicurezza online;
- ✓ Assicurare la protezione degli studenti e delle studentesse durante le attività che si svolgono insieme;
- ✓ Qualora si verificassero episodi che mettono in pericolo studenti e studentesse, segnalare al referente cyberbullismo e al/alla coordinatore/trice di classe.

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

GESTIONE DELLE INFRAZIONI ALLA *POLICY*

I provvedimenti includono le seguenti azioni:

- Qualsiasi rilevamento di sospetto di abuso, offesa, procurato disagio ricevuto su internet, sia personale che di un compagno, sarà sempre riferito, da parte del personale scolastico, al Dirigente Scolastico e al referente per il cyberbullismo, che fungeranno da primo punto di contatto;
- Possibile ritiro del cellulare fino a fine giornata;
- Saranno informati e documentati i genitori o i tutori per condividere con loro le strategie più opportune;
- Denunce di bullismo online saranno trattate in conformità con la legge attuale. Reclami relativi alla protezione dei minori saranno trattati in conformità alle procedure di protezione relative all'età specifica;
- Successivamente, nei casi più gravi, saranno avviate le comunicazioni alle autorità competenti;
- Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso. È bene ricordare a tutti che, nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia.

DISCIPLINA DEGLI ALUNNI

Potenziali infrazioni:

- ✓ Uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- ✓ Invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il numero di telefono;
- ✓ Condivisione di immagini intime;
- ✓ Comunicazione incauta e senza permesso con sconosciuti;
- ✓ Collegamento a siti web non indicati dai docenti.

Sono previsti da parte dei docenti provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento, quali:

- ✓ Richiamo verbale;
- ✓ Richiamo verbale con particolari conseguenze (riduzione o sospensione dell'attività gratificante);
- ✓ Richiamo scritto con annotazione sul diario;
- ✓ Convocazione dei genitori da parte degli insegnanti;
- ✓ Convocazione dei genitori da parte del Dirigente scolastico.

DISCIPLINA DEL PERSONALE SCOLASTICO

Comportamenti scorretti che sono da evitare:

- ✓ un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite l'installazione di software o tramite il salvataggio di materiali non idonei;
- ✓ un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- ✓ un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- ✓ una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- ✓ una carente istruzione preventiva degli alunni sull'utilizzazione corretta e responsabile delle tecnologie digitali e di internet;

DISCIPLINA DEI GENITORI

Le situazioni familiari meno favorevoli sono:

- ✓ la convinzione che se il proprio figlio rimane a casa ad usare il computer è al sicuro e non combinerà guai;
- ✓ una posizione del computer in una stanza o in un posto non visibile a tutti quando è utilizzato dal proprio figlio;
- ✓ una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo del cellulare o dello smartphone;
- ✓ un utilizzo del pc in comune con gli adulti che possono conservare in memoria materiali non idonei;
- ✓ un utilizzo del cellulare o dello smartphone in comune con gli adulti che possono conservare in memoria indirizzi o contenuti non idonei. I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli

DISCIPLINA DEGLI ALUNNI

Contestualmente sono previsti interventi di carattere educativo:

- ✓ di rinforzo dei comportamenti corretti;
- ✓ riparativi dei disagi causati;
- ✓ di ri-definizione delle regole sociali di convivenza attraverso 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 e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni.

DISCIPLINA DEL PERSONALE SCOLASTICO

- ✓ una vigilanza scarsamente attenta, che può favorire negli alunni un utilizzo non autorizzato delle TIC e possibili incidenti;

- ✓ interventi insufficienti:
  - ➢ nelle situazioni critiche di contrasto a terzi;
  - ➢ nella correzione e nel sostegno agli alunni;
  - ➢ nella segnalazione ai genitori, al Dirigente scolastico, all'animatore digitale.

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

Gestione accessi (password, backup, ecc.)

L'accesso al sistema informatico per la didattica (server e internet) nel laboratorio multimediale, è consentito al personale docente attraverso la registrazione presso il Collaboratore del Dirigente e l'Animatore digitale: la password è comune e consente di accedere al server. Non vi è un backup dei file elaborati, le postazioni del laboratorio funzionano come stazioni di lavoro e non come archivi.

E-mail L'account di posta elettronica è solo quello utilizzato ordinariamente da GSuite (cognome.nome@smsdomodossola.it), sia per la posta in ingresso che in uscita.

Blog e sito web della scuola La scuola attualmente ha un sito web. Tutti i contenuti del settore didattico sono pubblicati direttamente, previa valutazione del Dirigente scolastico che ne valuta la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

Social network Attualmente nella didattica si utilizzano i seguenti social network: Facebook, Instagram.

Protezione dei dati personali

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).

- ✓ 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 (**http://www.garanteprivacy.it/scuola**).

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

Nel nostro istituto 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).

Ai genitori è fornita l'informativa e la richiesta di autorizzazione all'utilizzo dei dati personali degli alunni, eccedenti i trattamenti istituzionali obbligatori.

L'Istituto allega alla presente *ePolicy* i modelli di liberatoria da utilizzare e conformi alla normativa vigente, in materia di protezione dei dati personali.

Strumentazione personale

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

Gestione degli strumenti personali – cellulari, tablet ecc.

ALUNNI

- ✓ L'uso di strumenti elettronici personali è consentito solo ed esclusivamente per scopi didattici[4];
- ✓ l'uso del cellulare[5]personale è consentito solo in caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione e con controllo dell'identità dell'interlocutore verificata dal docente.

[4]**ALLEGATO 5 -** Autorizzazione utilizzo device
[5]**ALLEGATO 4 –** Regolamento di disciplina e sanzioni/uso del cellulare (*Art.13/Regolamento d'Istituto*)

DOCENTI

- ✓ Durante le ore delle lezioni è consentito l'utilizzo del cellulare e/o di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili.
- ✓ Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

PERSONALE SCOLASTICO

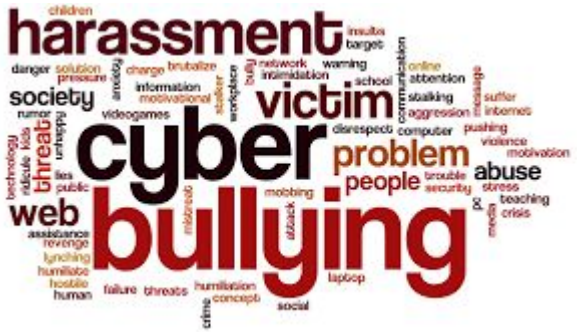
- ✓ Durante l'orario di servizio al restante personale scolastico è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente.

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 hai accesso;
- ✓ Rispettare la cosiddetta *netiquette* (regole condivise che disciplinano il rapportarsi fra utenti della rete, siti, forum, mail e di qualsiasi altro tipo di comunicazione).
- ✓ Controllo della validità e dell'origine delle informazioni a cui si accede o che si ricevono;
- ✓ Utilizzo di fonti alternative di informazione per proposte comparate;
- ✓ Ricerca del nome dell'autore, dell'ultimo aggiornamento del materiale e di altri possibili link al sito;
- ✓ Rispetto dei diritti di autore e dei diritti di proprietà intellettuale.

PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

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.

Strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio:

- ✓ **Sensibilizzazione:** fornire le informazioni necessarie (utili a conoscere il fenomeno) e illustrare le possibili soluzioni o i comportamenti da adottare.
- ✓ **Prevenzione:** 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.

Rischi nell'utilizzo delle TIC

➢ uso non corretto del telefono cellulare personale o dello smartphone o dei pc della scuola collegati alla rete.

Eludendo la sorveglianza degli insegnanti, gli alunni potrebbero scaricare e spedire foto personali o intime, proprie o di altri, video con contenuti indecenti o violenti, accedere a internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi.

COME PREVENIRE

- ✓ Informare e formare i docenti, i genitori, il personale ATA e gli studenti sui rischi che un uso non sicuro delle nuove tecnologie può favorire;
- ✓ Fornire ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori (es. liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi al proprio/a figlio/a);
- ✓ Non consentire l'utilizzo del cellulare personale degli alunni a scuola: per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola supervisionato dal personale addetto al centralino, che prima di passare la telefonata si accerta dell'identità dell'interlocutore;
- ✓ Consentire l'utilizzo del cellulare sono in casi particolari ed eccezionali, ad esempio quando ci si trova fuori dal contesto scolastico durante una visita guidata, e comunque sotto la supervisione dell'insegnante, che si accerta preventivamente dell'identità dell'interlocutore;
- ✓ Utilizzare filtri, software che impediscono il collegamento ai siti web per adulti (black list);
- ✓ Centralizzare il blocco dei siti web sul server del docente, utilizzando software che possono bloccare l'accesso ai siti internet semplicemente esaminando le varie richieste di connessione provenienti dai client collegati in rete locale, in modo tale che anche indipendentemente dal browser in uso su ciascuna macchina, il software sia capace di intercettare le richieste di collegamento e rigettare quelle che non rispettano le regole imposte dall'amministratore.

COME INTERVENIRE

- ✓ Se la condotta incauta dell'alunno consiste nel fare circolare immagini imbarazzanti, di natura sessuale, è necessario rimuoverle contattando il service provider;
- ✓ Se l'alunno viene infastidito od offeso, suggerirgli di modificare i dettagli del proprio profilo disponendolo su "privato", in modo tale che solo gli utenti autorizzati siano in grado di vederlo (MSN messenger, siti social network, Skype etc.), o suggerirgli di bloccare o ignorare particolari mittenti, di cancellare il loro nominativo dalla lista degli amici con i quali regolarmente chatta, di inserire il compagno o la persona che offende, per quanto riguarda l'e-mail, tra gli indesiderati;
- ✓ Consigliare di cambiare il proprio indirizzo e-mail, contattando l'email provider, di scaricare un'applicazione che blocchi chiamate e messaggi da numeri indesiderati o, se necessario, cambiare il numero di cellulare contattando l'operatore telefonico;
- ✓ Fare cancellare il materiale offensivo dal telefonino, facendo intervenire i genitori, e chiedere agli studenti di indicare a chi e dove lo hanno spedito per farlo fare anche gli altri, e conservare una copia di detto materiale per ulteriori indagini;
- ✓ Contattare la polizia se si ritiene che il materiale offensivo sia illegale. In caso di foto e video pedopornografici, confiscare il telefonino o altri dispositivi ed evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto, poiché ciò è reato per chiunque.

Cyberbullismo: 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".

➢ Le *Linee di orientamento per la prevenzione e il contrasto del cyberbullismo* prevedono:

- ✓ Formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- ✓ Sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- ✓ Promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- ✓ Previsione di misure di sostegno e rieducazione dei minori coinvolti;
- ✓ Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- ✓ Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.

Nomina del Referente per le iniziative di prevenzione e contrasto

- ✓ Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
- ✓ Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'Istituto), atti e documenti (PTOF, PdM, Rav).

➢ ***Gestione dei casi di "prepotenza" o "prevaricazione"***

I comportamenti definibili di "bullismo" possono esprimersi nelle forme più varie e non sono tratteggiabili a priori, se non contestualizzandoli. Le caratteristiche che aiutano a individuarli e a distinguerli dallo scherzo, dalle intemperanze caratteriali, dai diverbi usuali fra i ragazzi sono *la costanza nel tempo e la ripetitività, l'asimmetria* (disuguaglianza di forza e di potere), *il disagio della/e vittima/e.* Il bullismo si esplica infatti con comportamenti e atteggiamenti costanti e ripetitivi di arroganza, prepotenza, prevaricazione, disprezzo, dileggio, emarginazione, esclusione ai danni di una o più persone, agiti da un solo soggetto che generalmente è sostenuto da un gruppo.

Nel Cyber-bullismo, le molestie sono attuate attraverso strumenti tecnologici:

- invio di sms, messaggi in chat, e-mail offensive o di minaccia; diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o email nelle mailing-list o nelle chat-line;
- pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata. Il conflitto è da considerarsi come un campanello d'allarme e può degenerare in forme patologiche quando non lo si riconosce e non lo si gestisce in un'ottica evolutiva dei rapporti, di negoziazione e risoluzione. In considerazione dell'età degli alunni considerati, possono prefigurarsi alcune forme di interazioni che possono evolvere verso tale fenomeno. Per prevenire e affrontare il bullismo, i docenti non solo identificano vittime e prepotenti in divenire, ma tutti insieme affrontano e intervengono sul gruppo-classe, coinvolgendo i genitori degli allievi. L'elemento fondamentale per una buona riuscita dell'intervento educativo è infatti la corretta, compiuta e convinta ristrutturazione dell'ambiente sociale in cui tale fenomeno si verifica, e in particolare delle relazioni nel contesto della classe. Gli atteggiamenti degli alunni, così come quelli dei loro genitori, possono giocare un ruolo molto significativo nel ridurre la dimensione del fenomeno.

Gli interventi mirati sul gruppo classe sono gestiti in collaborazione dal team dei docenti della classe:

- ✓ attraverso percorsi di mediazione volta alla gestione positiva del conflitto, con gruppi di discussione (circle time), con rappresentazioni e attività di role-play sull'argomento del bullismo e del cyber-bullismo, con le strategie del problem solving;
- ✓ attraverso un questionario self-report da proporre agli studenti, con la finalità di indagare sulle situazioni a rischio;
- ✓ attraverso la reperibilità di una scheda di prima segnalazione del fenomeno presunto, reperibile online (sito della scuola – *cartella Generazioni Connesse*) e in cartaceo (presso la portineria, nel raccoglitore predisposto ai vari documenti di utilizzo); la scheda, una volta compilata, è da consegnare al referente del cyberbullismo.
- ✓ attraverso percorsi individualizzati di sostegno alle vittime, volti a incrementarne l'autostima e l'assertività e a potenziare le risorse di interazione sociale, mentre i prevaricatori sono destinatari di interventi mirati a smuoverne le competenze empatiche e a favorire una loro condivisione delle norme morali. Anche in relazione alle manifestazioni socio-affettive fra pari, al linguaggio sessualizzato o "volgare", al fine di evitare prevaricazioni e imbarazzo o disagio, i docenti intervengono per favorire nei loro alunni un buon rapporto con il proprio corpo e per far percepire meglio eventuali violazioni dei limiti di prossimità o di "confidenza" ed imparare ad opporvisi, per far acquisire fiducia nelle proprie sensazioni e nel proprio intuito, determinazione nel rifiutare i contatti anche "a distanza" sgradevoli o "strani", per rendere consapevoli gli alunni del diritto al rispetto dei propri limiti e di quelli altrui, per far capire ai ragazzi che l'interazione on-line deve sottostare a delle regole di buon comportamento. Inoltre la scuola, qualora rilevi una situazione psico-socio-educativa particolarmente problematica, convoca i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi. Consiglia altresì di servirsi dello **sportello di ascolto gratuito** attivo presso la scuola. Promuove e supporta la richiesta delle famiglie rivolta ai Servizi Sociali dell'Ente Locale per la fruizione di servizi socio-educativi comunali e alla ASL per quanto riguarda la competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare).

HATE SPEECH - “incitamento all’odio”: cos’è e come prevenirlo

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

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

- **Il discorso d'odio procura sofferenza.** La parola ferisce, e a maggior ragione l'odio! Il discorso può violare i diritti umani. Il discorso d'odio online non è meno grave della sua espressione offline, ma è più difficile da individuare e da combattere.
- **Gli atteggiamenti alimentano gli atti.** Il discorso dell'odio è pericoloso anche perché può condurre a più gravi violazioni dei diritti umani, e perfino alla violenza fisica. Può contribuire a inasprire le tensioni razziali e altre forme di discriminazione e di violenza.
- **L'odio online non è solo espresso a parole.** L'odio online può esprimersi sotto forma di video e foto, come pure, più solitamente, di contenuto testuale. Le forme visive o multimediali hanno sovente un impatto più forte sugli atteggiamenti (consci e inconsci).
- **L'odio prende di mira sia gli individui che i gruppi.** L'odio online può prendere di mira dei gruppi che spesso sono già vulnerabili sotto altri aspetti, come i richiedenti asilo, le minoranze religiose o le persone con disabilità. Tuttavia, anche i singoli individui sono sempre maggiormente oggetto di attacchi. Le conseguenze sono talvolta fatali, come dimostrato da numerosi fatti di cronaca riferiti dai media, riguardanti giovani vittime di cyberbullismo che sono state spinte al suicidio.
- **Internet è difficilmente controllabile.** La diffusione di messaggi di incitamento all'odio è maggiormente tollerata su Internet rispetto al mondo offline ed è sottoposta a minori controlli. È ugualmente più facile (e comporta meno rischi) insultare o molestare online, perché le persone spesso si esprimono sotto la copertura dell'anonimato.
- **Ha radici profonde.** Gli atteggiamenti e le tensioni sociali che suscitano sentimenti di odio online affondano le loro radici nella società, e non sono diversi, in genere, da quelli che alimentano il discorso dell'odio offline.
- **Impunità e anonimato.** Sono le due presunte caratteristiche delle interazioni sociali in rete: l'impunità e l'anonimato. Queste abbassano le remore etiche. In realtà, però, qualsiasi azione compiuta sul web consente di rintracciare il suo autore.

È utile prendere in considerazione alcuni aspetti:

- **Il contenuto e il tono**: certe espressioni di odio sono più estreme, utilizzano termini più insultanti e possono perfino istigare altri ad agire. All'altra estremità della scala, troviamo insulti più moderati o generalizzazioni eccessive, che presentano certi gruppi o individui sotto una cattiva (e perfino sotto falsa) luce.
- **L'intenzione degli autori degli insulti**: ci può capitare di offendere gli altri senza volerlo, e poi di pentircene, e perfino di ritirare quanto abbiamo detto; nell'hate speech l'intenzione degli autori è proprio quella di offendere e fare del male.
- **I bersagli o i bersagli potenziali**: alcuni gruppi, o individui, possono essere più vulnerabili di altri alle critiche. Può dipendere dal modo in cui sono globalmente considerati nella società, o da come sono rappresentati nei media, oppure dalla loro situazione personale, che non permette loro di difendersi efficacemente. La stessa espressione, applicata a gruppi diversi, può avere un impatto molto diverso.
- **Il contesto**: il contesto di una particolare espressione di odio è legato talvolta a circostanze storiche e culturali specifiche. Può includere altri fattori, come il mezzo utilizzato e il gruppo preso di mira, le tensioni o i pregiudizi esistenti, l'autorità del suo autore, etc.
- **L'impatto o l'impatto potenziale**: l'impatto reale o potenziale esercitato sugli individui, sui gruppi o sull'insieme della società è una delle principali considerazioni da tenere presenti. Spesso, le ripercussioni negative subite dall'individuo o dal gruppo si rivelano più importanti della valutazione dell'episodio da parte di osservatori esterni.

E' importante intervenire:

- ✓ organizzando uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.
- ✓ promuovendo incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

DIPENDENZA DA INTERNET E DAL GIOCO ONLINE

L'utilizzo eccessivo e incontrollato di Internet può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale.

Gli elementi che contribuiscono al benessere digitale sono:

- ✓ la ricerca di equilibrio nelle relazioni anche online;
- ✓ l'uso degli strumenti digitali per il raggiungimento di obiettivi personali;
- ✓ la capacità di interagire negli ambienti digitali in modo sicuro e responsabile;
- ✓ la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

COME PREVENIRE LA DIPENDENZA DA INTERNET E DAL GIOCO ONLINE

- Dedicare al tema un momento specifico e riflettere con studenti e studentesse per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.
- Integrare la tecnologia nella didattica, mostrando un suo utilizzo funzionale che possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online.
- Riflettere insieme su: come trascorri il tempo on line? Quando aggiunge valore alla tua vita e quando ti fa perdere tempo? Quale atteggiamento potresti cambiare quando sei online? Che ruolo ha e deve avere la tecnologia (internet o il gioco) nella tua vita?
- Parlare di **videogiochi,** pensandoli non in termini negativi ma di benessere digitale. Sono parte del mondo di studenti e studentesse. Riflettere insieme a ragazzi e ragazze su: quando sono una risorsa? Accedono a contenuti adeguati all'età? A che ora e per quanto tempo li usano? Diventa utile riflettere con i ragazzi e le ragazze rispetto all'uso della tecnologia in termini di **qualità e tempo:** se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi.
- Strutturare regole condivise e stipulare con loro una sorta di "patto" d'aula. È importante non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/lle studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.
- Proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d'aula.

SEXTING


SEXTING
SEXT
TEXTING
MESSAGE
DIRTY
SCHOOL
EDUCATION
SMS
RUDE
VALENTINE
PASSION
PHOTOGRAPH
EXOTIC
OBSESSION
AFFAIR
PERVERT
HARRASMENT
SEXUALLY
PRESSURE
INTERCOURSE
CONCERN
SEXY
MEDIA
SOCIAL
WARNING
LEGAL
RELATIONSHIP
EXPLICIT
NAKED
ISSUE
ONLINE
PARENTS
GENERATION
SEXUAL
SEND
KINKY
SURPRISE
OFFENSE
SEX
LOVERS
PICTURES
PHOTO
MOBILE
VIDEO
NUDE
LOVE
PORNOGRAPHIC
JUDGEMENT
SENSUAL
IMAGE
WRITTING
PHONE
PEER
VIRAL
BEHAVIOUR
DANGER

CARATTERISTICHE PRINCIPALI DEL FENOMENO

- **la fiducia tradita:** chi produce e invia contenuti sessualmente espliciti ripone fiducia nel destinatario, credendo, inoltre, alla motivazione della richiesta (es. prova d'amore richiesta all'interno di una relazione sentimentale);
- **la pervasività con cui si diffondono i contenuti:** in pochi istanti e attraverso una condivisione che diventa virale, il contenuto a connotazione sessuale esplicita può essere diffuso a un numero esponenziale e infinito di persone e ad altrettante piattaforme differenti. Il contenuto, così, diventa facilmente modificabile, scaricabile e condivisibile e la sua trasmissione è incontrollabile;
- **la persistenza del fenomeno:** 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 epoche successive.

CONSEGUENZE

- **"Revenge porn"**: 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, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti).
- La consapevolezza, o comunque la sola idea di diffusione di contenuti personali, si replica nel tempo e può finire con il danneggiare, sia in termini psicologici che sociali, sia il ragazzo/la ragazza soggetto della foto/del video che colui/coloro che hanno contribuito a diffonderla. Due agiti, quindi, che sono fra loro strettamente legati e che rappresentano veri e propri comportamenti criminali i quali hanno ripercussioni negative sulla vittima in termini di autostima, di credibilità, di reputazione sociale off e on line. A ciò si associano altri comportamenti a rischio, di tipo sessuale ma anche riferibili ad abuso di sostanze o di alcool.
- 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.

COME PREVENIRE

ADESCAMENTO ONLINE - GROOMING

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).

COME PREVENIRE

- ✓ 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.
- ✓ *Generazioni Connesse* ha realizzato un percorso con video interattivi per i/le ragazzi/e della scuola secondaria di primo grado (II e III classi) anche per affrontare il delicato tema dell'adescamento online (*es. Laura – Ep. 4 Web-serie "Se Mi Posti Ti Cancello").*
- ✓ È molto importante che ragazzi e ragazze sappiano a chi rivolgersi in caso di problemi, anche quando pensano di aver fatto un errore, si vergognano o si sentono in colpa. **Gli adulti coinvolti, genitori e docenti, devono essere un punto di riferimento per il minore che deve potersi fidare di loro e non sentirsi mai giudicato, ma compreso e ascoltato**. Affinché ciò avvenga è necessario tenere sempre aperto un canale di comunicazione con loro sui temi dell'affettività, del digitale e perché no, della sessualità.
- ✓ Fondamentale 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

COME INTERVENIRE

- ✓ 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 e delle Comunicazioni 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, inoltre, può essere una problematica molto delicata da gestire e può avere ripercussioni psicologiche significative sul minore. Per questo potrebbe essere necessario rivolgersi ad un Servizio territoriale (es. Consultorio Familiare, Servizio di Neuropsichiatria Infantile, ecc.) in grado di fornire alla vittima anche un adeguato supporto di tipo psicologico o psichiatrico.
- ✓ 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. Nei casi più estremi, in cui l'adescamento porta ad un incontro fisico e ad un abuso sessuale, un sostegno psicologico esperto per il minore è da considerarsi prioritario e urgente.
- ✓ Per consigli e per un supporto è possibile rivolgersi alla **Helpline di Generazioni Connesse (19696):** operatori esperti e preparati sono sempre a disposizione degli insegnanti, del Dirigente e degli operatori scolastici, oltre che dei bambini, degli adolescenti, dei genitori e di altri adulti che a vario titolo necessitano di un confronto e di un aiuto per gestire nel modo più opportuno eventuali esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media.

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.*

La pedopornografia è 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.

COME PREVENIRE	COME INTERVENIRE
✓ 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. L'educazione, compresa l'educazione all'affettività, riveste un ruolo fondamentale. ✓ E' importante sottolineare sempre la necessità di rivolgersi ad un adulto quando qualcosa online mette a disagio. ✓ E' importante svolgere un'attività di sensibilizzazione rivolta ai genitori e al personale scolastico, promuovendo i servizi delle hotline.	✓ Nel caso in cui una persona minorenne sia direttamente coinvolta nelle immagini, bisogna tenere in considerazione che l'attuale normativa (legge 172 del 2012, art. 351 c.p.p.) prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui la pedopornografia online, debba essere ascoltata dalle autorità competenti in sede di raccolta di sommarie informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

PROCEDURE OPERATIVE PER LA RILEVAZIONE, IL MONITORAGGIO E LA GESTIONE DELLE SEGNALAZIONI

CYBERBULLISMO: alcuni campanelli di allarme

Gli atti di bullismo avvengono prevalentemente entro o nei dintorni del contesto scolastico; tuttavia e in misura crescente le prepotenze vengono riportate nel contesto virtuale di internet. In queste situazioni si parla di *cyber-bullismo*, che si manifesta attraverso:

- invio di sms, mms, e-mail offensivi/e o di minaccia;
- diffusione di messaggi offensivi ai danni della vittima, attraverso la divulgazione di sms o email nelle mailing-list o nelle chat-line;
- pubblicazione nel cyberspazio di foto o filmati che ritraggono prepotenze o in cui la vittima viene denigrata.

La rilevazione diretta o indiretta degli indicatori da parte degli insegnanti, sulla base di quanto riferito dagli alunni o dai genitori, deve affinarsi con l'osservazione delle relazioni interpersonali e delle possibili dinamiche conflittuali sottostanti presenti nel contesto classe, al fine di verificare l'entità e la natura del fenomeno e dare avvio al programma di intervento.

A chi segnalare: l'attuazione del programma di intervento si basa prevalentemente sull'impiego delle risorse umane già presenti e disponibili: il referente al cyberbullismo, tutti i docenti e il personale scolastico, alunni e genitori, servizio dello sportello di ascolto. Non serve, se non in casi particolarmente gravi, l'opera di psicologi, assistenti sociali o altri specialisti a cui orientare la famiglia. L'elemento fondamentale per una buona riuscita del programma è infatti la corretta ristrutturazione del

ABUSI SESSUALI: alcuni campanelli di allarme

Internet ha ampliato le possibilità di abuso sessuale dei minori: permette di scaricare o vendere immagini o filmati di pornografia infantile (pedopornografia), in cui le vittime sono appunto i minori. Inoltre, succede che un adulto prenda contatto con dei bambini nei forum o nelle chat su internet, e che li metta di fronte a domande o messaggi sessuali o addirittura a immagini pornografiche. A volte l'adulto induce i bambini a spogliarsi davanti alla webcam oppure a inviare una fotografia che li ritrae nudi tramite internet o sul cellulare.
L'osservazione della presenza dei suddetti indicatori da parte degli insegnanti deve essere attenta e pronta alla segnalazione.

A chi segnalare: nel caso in cui ci si dovesse imbattere in materiale pedopornografico (cioè contenuti foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali), è necessario, innanzitutto, evitare di eseguire download, produrne copie, condividerne link o postarne il contenuto. Ciò è reato per chiunque. Nel venire a conoscenza di materiali di questo tipo è importante contribuire alla loro eliminazione: basta inserire le informazioni richieste sugli appositi moduli online, disponibili al sito **http://www.azzurro.it/it/clicca-e-segnala"** ovvero collegandosi al sito della polizia postale **https://www.commissariatodips.it**, ove è possibile sia segnalare che denunciare. In alternativa è possibile recarsi nella sede più vicina della polizia giudiziaria. Ciò consente di operare con la massima tempestività. È bene non operare in modo isolato, ma confrontarsi con i colleghi di

GLI ATTORI SUL TERRITORIO

Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.
Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di **Generazioni Connesse** *"Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani"* (seconda parte, pag. 31), senza dimenticare che la **Helpline** di **Telefono Azzurro (19696)** è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

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

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

Nella prevenzione e nel contrasto alle varie forme di abuso che possono verificarsi sulla piattaforma online e non solo, la Scuola attua ricorrenti forme di collaborazione:

- con le Forze dell'ordine: Polizia Municipale, Arma dei Carabinieri, Polizia Postale (incontri e conferenze rivolti a tutti gli attori del processo educativo);
- con le associazioni presenti sul territorio, attraverso la proposta di rappresentazioni (es. teatrali) e laboratori agli studenti e alle studentesse.

Siti utili

http://www.azzurro.it/it

https://www.generazioniconnesse.it/

https://www.commissariatodips.it/

Generazioni Connesse
SAFER INTERNET CENTRE

LINEE GUIDA PER GLI ALUNNI

1. Non comunicare mai a nessuno la tua password e cambiala periodicamente, usando numeri, lettere e caratteri speciali;
2. Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo della tua scuola;
3. Non inviare a nessuno fotografie tue o di tuoi amici;
4. Prima di inviare o pubblicare su un BLOG la fotografia di qualcuno, chiedi sempre il permesso;
5. Chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da Internet;
6. Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di riferire l'indirizzo della tua scuola;
7. Quando sei connesso alla rete RISPETTA SEMPRE GLI ALTRI: ciò che per te è un gioco può rivelarsi offensivo per qualcun altro;
8. Non rispondere alle offese e agli insulti;
9. Blocca i Bulli: molti Blog e siti social network ti permettono di segnalare i cyber-bulli;
10. Conserva le comunicazioni offensive, potrebbero essere utili per dimostrare quanto ti è accaduto;
11. Se ricevi materiale offensivo (e-mail, sms, mms, video, foto, messaggi vocali) non diffonderlo: potresti essere accusato di cyber-bullismo;
12. Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE;
13. Se qualcuno ti invia immagini che ti infastidiscono, non rispondere: riferisci al tuo insegnante o ai tuoi genitori. Riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet;
14. Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori;
15. Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere;
16. Non è consigliabile inviare mail personali, perciò rivolgiti sempre al tuo insegnante prima di inviare messaggi di classe o ai tuoi genitori prima di inviare messaggi da casa;
17. Non scaricare (download) o copiare materiale da Internet senza il permesso del tuo insegnante o dei tuoi genitori;
18. Non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso del tuo insegnante o dei tuoi genitori.

LINEE GUIDA PER I DOCENTI

1. Evitate di lasciare le e-mail o i file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune;
2. Salvate sempre i vostri lavori (file) in cartelle personali e/o di classe e non sul desktop o nella cartella del programma in uso. Sarà cura di chi mantiene il corretto funzionamento delle macchine cancellare file di lavoro sparsi sul computer e al di fuori delle cartelle personali;
3. Discutete con gli alunni della policy e-safety della scuola, dell'utilizzo consentito della rete e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet;
4. Date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni saranno monitorate;
5. Ricordate di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione su Internet del laboratorio (qualora sia stata attivata);
6. Ricordate agli alunni che la violazione consapevole della policy e-safety della scuola, di utilizzo consentito della rete, comporta sanzioni di diverso tipo;
7. Adottate provvedimenti "disciplinari" proporzionati all'età e alla gravità del comportamento;
8. Adottate interventi di carattere educativo di rinforzo dei comportamenti corretti e riparativi, di ri-definizione delle regole sociali di convivenza attraverso 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 e di reti di solidarietà, di promozione della conoscenza e della gestione delle emozioni;
9. Nelle situazioni psico-socio-educative particolarmente problematiche, convocate i genitori o gli esercenti la potestà per valutare con loro a quali risorse territoriali possono rivolgersi (Sportello di ascolto gratuito attivo presso la scuola, Servizi Sociali per la fruizione di servizi socio educativi comunali, ASL per quanto riguarda la competenza psicologica e psicoterapeutica: Pediatria, Neuropsichiatria infantile, Consultorio Familiare);
10. Chiedete/suggerite di cancellare il materiale offensivo, di bloccare o ignorare particolari mittenti, di uscire da gruppi non idonei, di cambiare indirizzo e-mail, ecc... ;
11. Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro;
12. In caso di abuso sessuale, rilevato anche attraverso i nuovi mezzi di comunicazione come internet o il cellulare, confrontatevi con i colleghi di classe e il Dirigente Scolastico.

CONSIGLI AI GENITORI
PER UN USO RESPONSABILE DI INTERNET A CASA

Consigli generali

- ✔ Posizionate il computer in una stanza accessibile a tutta la famiglia;
- ✔ Evitate di lasciare le e-mail o file personali sui computer di uso comune;
- ✔ Concordate con vostro figlio le regole: quando si può usare internet e per quanto tempo.
- ✔ Inserite nel computer i filtri di protezione: prevenite lo spam, i pop-up pubblicitari, l'accesso a siti pornografici;
- ✔ Aumentate il filtro del "**parental control**" attraverso la sezione *sicurezza in internet* dal pannello di controllo;
- ✔ Attivate il firewall (protezione contro malware) e antivirus;
- ✔ Mostratevi coinvolti: chiedete a vostro figlio di mostrarvi come funziona internet e come viene usato per scaricare e caricare compiti, lezioni, materiali didattici e per comunicare con l'insegnante;
- ✔ Incoraggiate le attività on-line di alta qualità: ricercare informazioni scientifiche, ricercare nuovi amici nel mondo;
- ✔ Partecipate alle esperienze on-line: navigate insieme a vostro figlio, incontrate amici on-line, discutete gli eventuali problemi che si possono presentare;
- ✔ Comunicate elettronicamente con vostro figlio: inviate, frequentemente, Email, Instant Messenger;
- ✔ Spiegate a vostro figlio che la password per accedere ad alcune piattaforme è strettamente personale e non deve essere mai fornita ai compagni o ad altre persone;
- ✔ Stabilite ciò che ritenete inaccettabile (razzismo, violenza, linguaggio volgare, pornografia);
- ✔ Discutete sul tema dello scaricare file e della possibilità di ricevere file con virus;
- ✔ Raccomandate di non scaricare file da siti sconosciuti;
- ✔ Incoraggiate vostro figlio a dirvi se vede immagini particolari o se riceve e-mail indesiderate;
- ✔ Discutete nei dettagli le conseguenze che potranno esserci se vostro figlio visita deliberatamente siti non adatti, ma non rimproveratelo se compie azioni involontarie;
- ✔ Spiegate a vostro figlio che le password, i codici pin, i numeri di carta di credito e i numeri di telefono e i dettagli degli indirizzi e-mail sono privati e non devono essere dati ad alcuno;
- ✔ Spiegate a vostro figlio che non tutti in Internet sono realmente *chi* dichiarano di essere; di conseguenza, i vostri ragazzi non dovrebbero mai accordarsi per appuntamenti senza consultarvi;
- ✔ Il modo migliore per proteggere i vostri ragazzi è usare Internet con loro, discutere e riconoscere insieme i rischi potenziali.

Consigli in base all'età

Se tuo figlio ha meno di 8 anni

Seleziona con molta attenzione i siti "sicuri": ricordati che i gestori dei siti, per trarre il massimo guadagno, permettono agli inserzionisti di pubblicizzare i propri prodotti; comunica a tuo figlio tre semplici regole:

- ✔ non dare il tuo vero nome, indirizzo e numero di telefono. Usa sempre il tuo "computer username" o nickname;
- ✔ se compare sullo schermo qualche messaggio /banner, chiudilo: insegna a tuo figlio come si fa;
- ✔ naviga esclusivamente sui siti autorizzati dai genitori, (molti siti richiedono la registrazione. Insegna a tuo figlio come registrarsi senza rivelare informazioni personali).

Se tuo figlio ha tra gli 8 anni e i 10 anni

- ✔ Progressivamente diminuisci la supervisione: dagli otto ai dieci anni permetti a tuo figlio di navigare da solo nei siti autorizzati, sottolineando che deve consultarti prima di esplorarne dei nuovi.
- ✔ Verifica periodicamente i contenuti dei siti "sicuri".
- ✔ Discuti con tuo figlio i rischi che possono presentarsi durante la navigazione on-line.
- ✔ Dalla cronologia, controlla il menu navigazione per verificare se tuo figlio ha consultato siti non autorizzati, per i quali non ti ha chiesto il permesso.
- ✔ Supervisiona l'e-mail di tuo figlio, dopo averlo reso consapevole del fatto che hai pieno accesso alle sue comunicazioni.
- ✔ Se tuo figlio vuole usare IM (messaggistica istantanea), verifica che i suoi contatti siano limitati agli amici conosciuti. Specifica che non può inserire nuovi contatti senza averti prima consultato.
- ✔ Comunicagli che è assolutamente vietato cliccare su un link, contenuto in una E-mail, su un pop-up pubblicitario o su un banner (ricordati, infatti, che potrebbero presentarsi immagini pornografiche o che potrebbe avviarsi il download di "malware").
- ✔ Incoraggia l'uso di internet per svolgere ricerche scolastiche. Definisci il tempo massimo di connessione ed incoraggia le attività con il mondo reale.

Se tuo figlio ha tra gli 11 anni e i 13 anni

Tuo figlio è diventato grande e potrebbe dirti che il suo migliore amico ha la possibilità di navigare tutti i giorni e a tutte le ore …. Che fare?

- ✔ Crea una partnership con i genitori dei migliori amici di tuo figlio in modo da concordare con loro le regole: tempi di connessione, fasce orarie, siti autorizzati, modalità di utilizzo di IM (messaggistica istantanea).
- ✔ Aiuta tuo figlio a creare una rete on-line sicura: siti controllati ed amici conosciuti.

Se tuo figlio ha oltre 13 anni

- ✔ Verifica i profili di tuo figlio e dei suoi amici nei siti cerca persona, informandolo dei tuoi periodici controlli. Ricordati che in questa fascia di età aumentano le ricerche di materiale sessuale ed i rischi di seduzioni sessuali online da parte di cyber-predatori adulti: condividi con tuo figlio le procedure per navigare in sicurezza ed evitare on-line e off-line brutti incontri.
- ✔ Confrontati con tuo figlio su tutti questi rischi: se lui protesta per il controllo, ribadisci che è un dovere del genitore supervisionare e monitorare l'uso di internet.
- ✔ Stringi un accordo: se tuo figlio dimostra di avere compreso i rischi, e di sapere e volere usare internet in modo sicuro, diminuisci la supervisione.
- ✔ Il computer deve rimanere in una stanza accessibile a tutta la famiglia, e non nella camera di tuo figlio, ALMENO fino ai 16 anni.

ELENCO ALLEGATI
E- Safety Policy Integrale

- **ALLEGATO 1 – Patto di Corresponsabilità**
- **ALLEGATO 2: - Regolamento ambienti di apprendimento online e dispositivi digitali**
- **ALLEGATO 3: - Dichiarazione di assunzione di responsabilità da parte degli studenti/genitori**
- **ALLEGATO 4 - Regolamento di disciplina e sanzioni / uso del cellulare** *(Art. 13 dal Regolamento d'Istituto)*
- **ALLEGATO 5 - Autorizzazione utilizzo device**
- **ALLEGATO 6 - Questionario self report sul bullismo**
- **ALLEGATO 7 - Questionario self report sul cyberbullismo**
- **ALLEGATO 8 - Scheda di prima segnalazione su presunti fenomeni di bullismo e cyberbullismo**
- **ALLEGATO 9 - Scheda di richiesta intervento del garante per la protezione dei dati**
- **ALLEGATO 10 - Procedure di segnalazione Enti esterni**