IT GARIBALDI DA VINCI
CESENA

Documento di E-policy

I.T. "GARIBALDI/DA VINCI"

FOTA03000R

VIA SAVIO 2400 - 47522 - CESENA - FORLI'-CESENA (FO)

Dirigente scolastica Prof.ssa Luciana Cino

A cura del gruppo di lavoro
"Bullismo e cyberbullismo"

Prof.ssa Giulia Fiumana
Prof.ssa Silvia Mosconi
Prof.ssa Anna Puca
Prof.ssa Cinzia Sirri
Prof.ssa Anna Maria Stroppolo

Indice

5) Segnalazione e gestione dei casi

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

Capitolo 1
Presentazione dell'E-policy

1.1 Scopo dell'E-policy

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

Le "competenze digitali" sono fra le abilità chiave all'interno del Quadro di riferimento Europeo delle Competenze per l'apprendimento permanente (Raccomandazione del Consiglio Europeo del 2006 aggiornata al 22 maggio 2018, relativa alle competenze chiave per l'apprendimento permanente).

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

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

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.
L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

.

1.2 Ruoli e responsabilità

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

Dirigente scolastico

Il ruolo del Dirigente scolastico nel promuovere l'uso consentito delle tecnologie e di internet include i seguenti compiti:

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

Animatore digitale

Il ruolo dell'Animatore digitale include i seguenti compiti:

- ✓ stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;

- ✓ monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, 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".

Direttore dei servizi generali e amministrativi

Il ruolo del direttore dei servizi generali e amministrativi include i seguenti compiti:

- ✓ 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 degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Docenti

Il ruolo del personale docente e di ogni figura educativa che lo affianca include i seguenti compiti:

- ✓ informarsi/aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- ✓ garantire che 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 sul diritto 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;
- ✓ 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;
- ✓ 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 di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- ✓ segnalare al Dirigente scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

Alunni

Il ruolo degli alunni include i seguenti compiti:

- ✓ essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;
- ✓ avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche 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 per non correre rischi;

- ✓ adottare condotte rispettose degli altri anche quando si comunica in ete;
- ✓ esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

Genitori

Il ruolo dei genitori degli alunni include i seguenti compiti:

- ✓ 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 del telefonino in generale.

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

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

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

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

1.4 Condivisione e comunicazione dell'E-policy all'intera comunità scolastica

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

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

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

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

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

1.5 Gestione delle infrazioni all'E-policy

Disciplina degli studenti

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.

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

- ✓ un uso della rete per giudicare, infastidire o impedire a qualcuno di esprimersi o partecipare;
- ✓ l'invio incauto o senza permesso di foto o di altri dati personali come l'indirizzo di casa o il telefono;
- ✓ la condivisione di immagini intime o troppo spinte;
- ✓ la comunicazione incauta e senza permesso con sconosciuti;
- ✓ il collegamento a siti web non indicati dai docenti. Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo dell'alunno. Infatti più gli alunni sono piccoli, più i comportamenti "da correggere" sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, che devono essere compresi e orientati proprio dagli educatori, nella prospettiva del raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

Sono previsti pertanto da parte dei docenti provvedimenti “disciplinari” proporzionati all’età e alla gravità del comportamento, quali:

- ✓ il richiamo verbale;
- ✓ il richiamo verbale con particolari conseguenze (riduzione o sospensione dell’attività gratificante);
- ✓ il richiamo scritto con annotazione sul diario;
- ✓ la convocazione dei genitori da parte degli insegnanti;
- ✓ la convocazione dei genitori da parte del Dirigente scolastico.

Contestualmente sono previsti interventi di carattere educativo di rinforzo dei comportamenti corretti e 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

Le potenziali infrazioni in cui è possibile che il personale scolastico e in particolare i docenti incorrano nell’utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull’uso corretto e responsabile delle TIC da parte degli alunni:

- ✓ 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 installazione di software o 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;
- ✓ una vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;

- ✓ insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di 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.

Tutto il personale è tenuto a collaborare con il Dirigente scolastico e a fornire ogni informazione utile per le valutazioni del caso 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.

Disciplina dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.
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 altri.

1.6 Integrazione dell'E-policy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico verrà aggiornato nell'anno scolastico 2020/21 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.

1.7 Monitoraggio dell'implementazione dell'E-policy e suo aggiornamento

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

Il nostro piano d'azione prevede di organizzare

- ✓ entro un anno, 2 eventi di presentazione
  - 1 del progetto Generazioni Connesse rivolto agli studenti
  - 1 dell'E-policy rivolto ai docenti
- ✓ nei prossimi 3 anni,
  - incontri per la consultazione degli studenti/studentesse sui temi dell'E-policy per cui si evidenzia la necessità di regolamentare azioni e comportamenti
  - 1 evento di presentazione del progetto Generazioni Connesse rivolto ai docenti.

Capitolo 2
Formazione e curricolo

2.1 Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".
Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).
Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

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.
Il corpo docente ha partecipato a corsi di formazione anche nell'ambito di piani nazionali, oltre che ad iniziative organizzate dall'istituzione o dalle scuole associate in rete e possiede generalmente sufficienti competenze e nel caso delle figure di sistema, anche di carattere specialistico. È inoltre disponibile ad aggiornarsi per mantenere al passo la propria formazione, in rapporto al rinnovo della dotazione multimediale. Il percorso complesso della formazione

specifica dei docenti sull'utilizzo delle TIC nella didattica, non esauribile nell'arco di un anno scolastico, può pertanto prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore digitale, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo; può comprendere altresì la fruizione dei materiali messi a disposizione dall'Animatore stesso sulle bacheche virtuali appositamente create, corsi di aggiornamento online.

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

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

2.4 Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

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

2.5 Il nostro Piano d'azione

Le azioni attuate nell'a.s. 2019/20 sono le seguenti:

- ✓ effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica;
- ✓ effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali;
- ✓ organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica;
- ✓ organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali;
- ✓ organizzare incontri con esperti per i docenti sulle competenze digitali.

Le azioni che si prevede di sviluppare nei tre anni successivi sono le seguenti:

- ✓ effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- ✓ effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- ✓ effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- ✓ coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- ✓ organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- ✓ organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- ✓ organizzare incontri con esperti per i docenti sulle competenze digitali.

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

3.1 Protezione dei dati personali

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

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

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

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

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

3.2 Accesso ad internet

L'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, (commissione costituita nel 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà) recita

L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.
Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.
Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.
L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.
Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.

Il 30 aprile 2016 è entrato poi in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che ha stabilito le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".
Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".
Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.
In particolare rispetto all'utilizzo del Laboratorio di INFORMATICA, delle postazioni di lavoro e dell'uso di internet, si danno le seguenti disposizioni:

Disposizioni sull'uso del laboratorio

- ✓ Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
- ✓ I laboratori informatici e le postazioni informatiche dell'istituto possono essere utilizzati esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
- ✓ Quando un insegnante, da solo o in classe, usufruisce del laboratorio deve obbligatoriamente registrare il proprio nome e l'eventuale classe nell'apposito registro delle presenze di laboratorio, indicando l'orario di ingresso, quello di uscita e motivazione dell'uso delle postazioni informatiche. Questo allo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula.
- ✓ L'ingresso degli allievi nei laboratori è consentito solo in presenza dell'insegnante.
- ✓ Il docente accompagnatore è responsabile del corretto uso didattico di hardware e software.
- ✓ Nei laboratori è vietato utilizzare CD personali o dischetti se non dopo opportuno controllo con sistema di antivirus aggiornato
- ✓ È vietato cancellare o alterare files-dati presenti sull'hard disk.
- ✓ Il laboratorio non deve mai essere lasciato aperto o incustodito quando nessuno lo utilizza. All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il mobilio in ordine, le macchine spente correttamente (chiudi sessione…).
- ✓ In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.
- ✓ In caso di malfunzionamento non risolvibile dal responsabile di laboratorio si contatterà personalmente o attraverso il Responsabile di laboratorio, la segreteria.
- ✓ Per motivi di manutenzione straordinaria, in caso di guasti o di virus, i PC possono essere formattati senza preavviso. Si consiglia pertanto di salvare i dati importanti su Cd o pen drive periodicamente. In caso di formattazione ordinaria ci sarà un preavviso.

Disposizioni sull'uso dei software

- ✓ I software installati sono ad esclusivo uso didattico.
- ✓ In base alle leggi che regolano la distribuzione delle licenze, i prodotti software presenti in laboratorio non sono disponibili per il prestito individuale. Nei casi in cui lo fossero in base a precise norme contrattuali i docenti interessati, dopo aver concordato il prestito con il Responsabile di laboratorio, devono compilare l'apposito registro di consegna software custodito in laboratorio.

- ✓ È fatto divieto di usare software non conforme alle leggi sul copyright. È cura dell'insegnante utente di verificarne la conformità. Gli insegnanti possono installare nuovo software sui PC del laboratorio della propria scuola, previa autorizzazione scritta del DS solo se il software installato rispetta le leggi sul copyright.
- ✓ È responsabilità degli insegnanti che chiedono al Responsabile di laboratorio di effettuare copie di cd/dvd per uso didattico, di assicurarsi che la copia non infranga le leggi sul copyright in vigore.

Accesso a internet

- ✓ L'accesso a Internet è consentito al personale docente e non docente solo ad esclusivo uso didattico e/o di formazione e alle classi accompagnate 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, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.
- ✓ Il Responsabile di laboratorio che verifichi un uso del laboratorio contrario a disposizioni di legge o del regolamento interno deve darne comunicazione per iscritto al Dirigente Scolastico.

3.3 Strumenti di comunicazione online

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

3.4 Strumentazione personale

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

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

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

3.5 Il nostro Piano d'azione

Le azioni che sono state attuate nel corso dell'a.s. 2019/20 sono le seguenti:

- ✓ effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte degli studenti e delle studentesse;
- ✓ effettuare un'analisi sull'utilizzo dei dispositivi personali a scuola da parte dei docenti.

Le azioni da sviluppare nell'arco dei tre anni successivi sono le seguenti:

- ✓ Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity).

Capitolo 4
Rischi on line: conoscere, prevenire e rilevare

4.1 Sensibilizzazione e prevenzione

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

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

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

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

4.2 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".

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

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

4.3 Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena.

Più ampiamente il termine “hate speech” indica un’offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.
Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l’obiettivo di:

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

Durante le lezioni, principalmente di italiano, religione e alternativa alla religione si affronteranno queste tematiche per mezzo di visione di video e condivisione di esperienze.

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’istituto è intenzionato a promuovere azioni di prevenzione attraverso i percorsi sul benessere digitale promossi dalla Ausl di Cesena o attraverso l’azione educativa dei singoli docenti durante le lezioni.

4.5 Sexting

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

Durante le lezioni, principalmente di italiano, religione e alternativa alla religione si affronteranno queste tematiche per mezzo di visione di video e condivisione di esperienze.

4.6 Adescamento on line

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).

Durante le lezioni, principalmente di Lingua e letteratura italiana, Religione/Alternativa alla religione si affronteranno queste tematiche per mezzo di visione di video e condivisione di esperienze.

4.7 Pedopornografia

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

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

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

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

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

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

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

Durante le lezioni, principalmente di italiano, religione e alternativa alla religione si affronteranno queste tematiche per mezzo di visione di video e condivisione di esperienze.

Capitolo 5
Segnalazione e gestione dei casi

5.1 Cosa segnalare

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

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

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

Nelle procedure:

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

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

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

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

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

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

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

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

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

5.2 Come segnalare; quali strumenti e a chi

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

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

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

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

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

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

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

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

5.3 Gli attori sul territorio

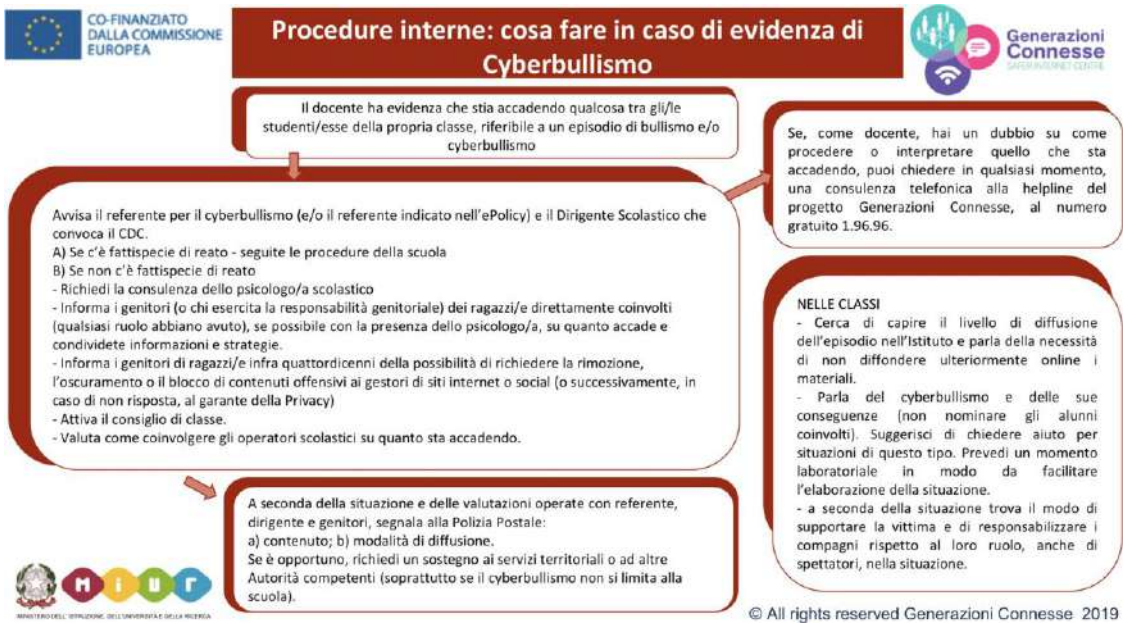
Talvolta, nella gestione dei casi, può essere necessario rivolgersi **ad altre figure, enti, istituzioni e servizi presenti sul territorio** qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.
A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

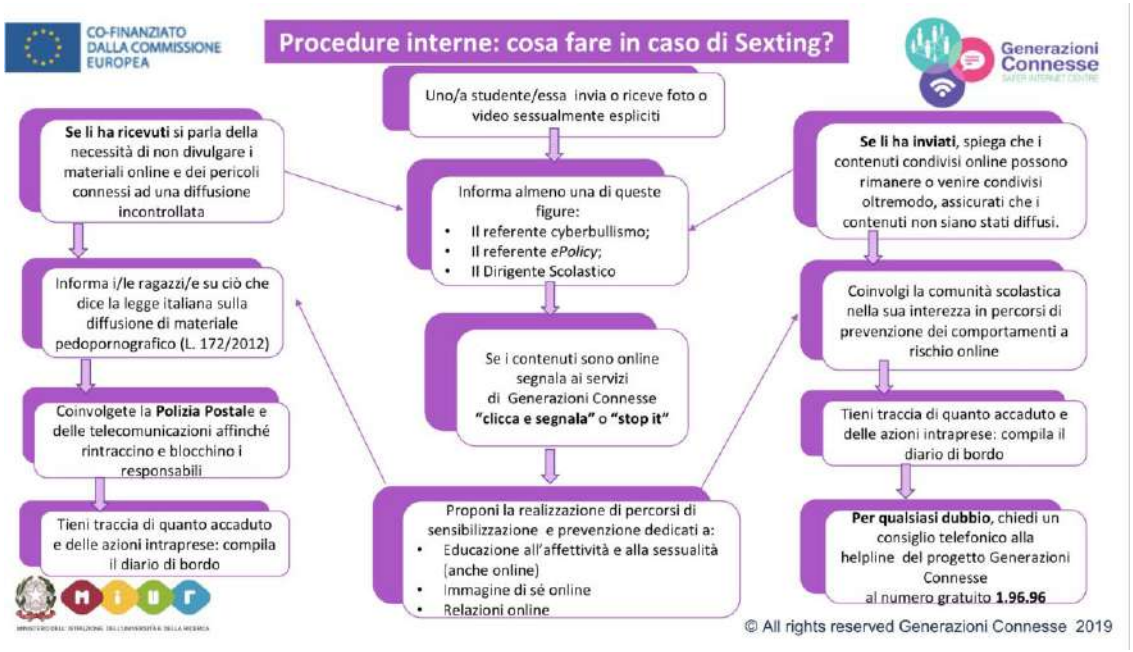
- ✓ Comitato Regionale Unicef: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- ✓ Co.Re.Com. (Comitato Regionale per le Comunicazioni): svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare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

5.4 Allegati con le procedure

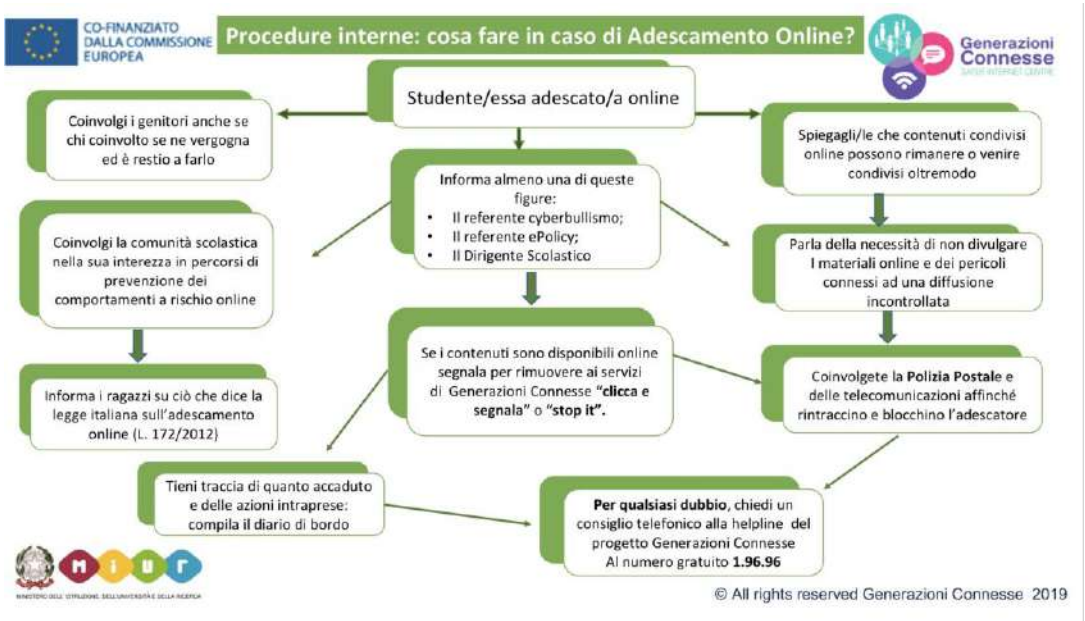
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



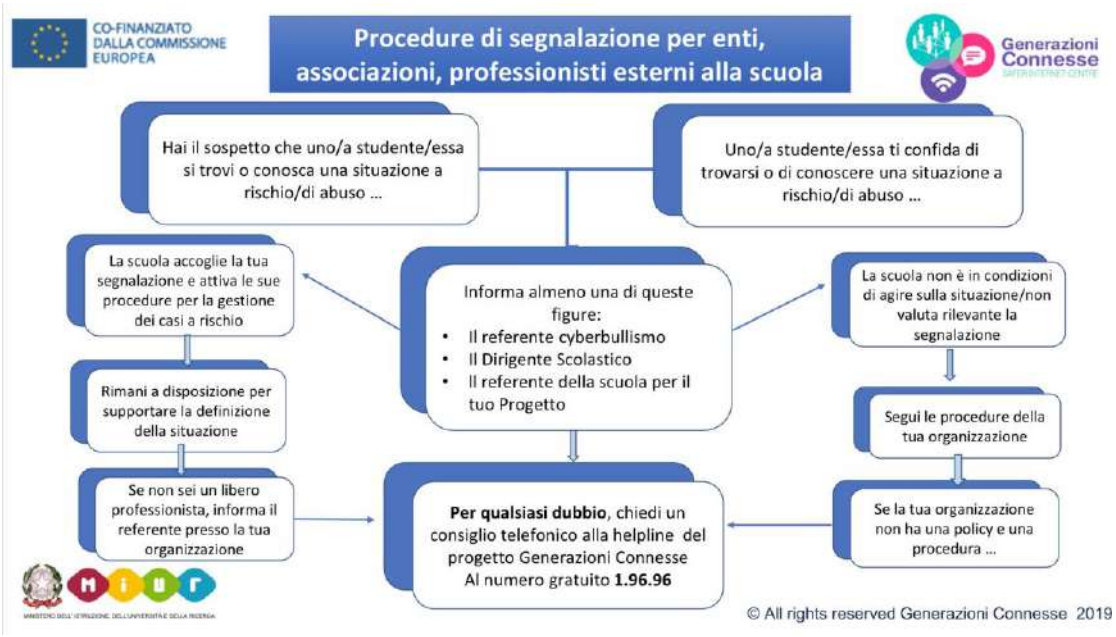
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

LINEE GUIDA PER ALUNNI

- ✓ Non comunicare mai a nessuno la tua password e periodicamente cambiala, usando numeri, lettere caratteri speciali;
- ✓ Mantieni segreto il nome, l'indirizzo, il telefono di casa, il nome e l'indirizzo
- ✓ della tua scuola;
- ✓ Non inviare a nessuno fotografie tue o di tuoi amici;
- ✓ Prima di inviare o pubblicare su un BLOG la fotografia di qualcuno, chiedi sempre il permesso;
- ✓ Chiedi sempre al tuo insegnante a scuola o ai tuoi genitori a casa il permesso di scaricare documenti da Internet;
- ✓ Chiedi sempre il permesso prima di iscriverti a qualche concorso o prima di
- ✓ riferire l'indirizzo della tua scuola;
- ✓ Quando sei connesso alla rete RISPETTA SEMPRE GLI ALTRI, ciò che per te è un gioco può rivelarsi offensivo per qualcun altro;
- ✓ Non rispondere alle offese ed agli insulti;
- ✓ Blocca i Bulli: molti Blog e siti social network ti permettono di segnalare i cyberbulli;
- ✓ Conserva le comunicazioni offensive, ti potrebbero essere utili per dimostrare quanto ti è accaduto;
- ✓ Se ricevi materiale offensivo (e-mail, sms, mms, video, foto, messaggi vocali) non diffonderlo: potresti essere accusato di cyberbullismo;
- ✓ Rifletti prima di inviare: ricordati che tutto ciò che invii su internet diviene pubblico e rimane per SEMPRE;
- ✓ Riferisci al tuo insegnante o ai tuoi genitori se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet;
- ✓ Se qualcuno su Internet ti chiede un incontro di persona, riferiscilo al tuo insegnante o ai tuoi genitori;
- ✓ Ricordati che le persone che incontri nella Rete sono degli estranei e non sempre sono quello che dicono di essere;

- ✓ Non è consigliabile inviare mail personali, perciò rivolgiti sempre al tuo docente prima di inviare messaggi di classe o ai tuoi genitori prima di inviare messaggi da casa;
- ✓ Non scaricare (download) o copiare materiale da Internet senza il permesso del tuo docente o dei tuoi genitori;
- ✓ Non caricare (upload) materiale video o fotografico nei siti web dedicati senza il permesso del tuo docente o dei tuoi genitori.

LINEE GUIDA PER INSEGNANTI

- ✓ Evitate di lasciare le e-mail o file personali sui computer o sul server della scuola, lo spazio è limitato e di uso comune;
- ✓ 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 per la macchina e al di fuori delle cartelle personali;
- ✓ Discutete con gli alunni della policy e-safety della scuola, di utilizzo consentito della rete, e degli eventuali problemi che possono verificarsi nell'applicazione delle regole relative all'uso di Internet;
- ✓ Date chiare indicazioni su come si utilizza Internet, ed eventualmente anche la posta elettronica, e informateli che le navigazioni saranno monitorate;
- ✓ 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);
- ✓ Ricordate agli alunni che la violazione consapevole della policy e-safety della scuola, di utilizzo consentito della rete, comporta sanzioni di diverso tipo;
- ✓ Adottate provvedimenti "disciplinari", proporzionati all'età e alla gravità del
- ✓ Comportamento;
- ✓ 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;
- ✓ 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 psicologico gratuito attualmente attivo presso la scuola, Servizi Sociali per la fruizione di servizi socio- educativi comunali, ASL per quanto di competenza psicologica e psicoterapeutica (Pediatria, Neuropsichiatria infantile, Consultorio Familiare);
- ✓ Chiedete/suggerite di cancellare il materiale offensivo, bloccare o ignorare particolari mittenti, uscire da gruppi non idonei, cambiare indirizzo e-mail, ecc...;

- ✓ Segnalate la presenza di materiale pedopornografico (senza scaricarlo o riprodurlo) alla Polizia Postale o al Telefono Azzurro;
- ✓ 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 salone o 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 controll" 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;
- ✓ Partecipa alle esperienze on-line: naviga insieme a tuo figlio, incontra amici on-line, discuti gli eventuali problemi che si presentano;
- ✓ Comunicate elettronicamente con vostro figlio: inviate, frequentemente, E- mail, Instant Message;
- ✓ 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 vedono immagini particolari o se ricevono 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 chi realmente dichiarano di essere; di conseguenza i vostri ragazzi non dovrebbero mai accordarsi per appuntamenti senza consultarvi prima;
- ✓ Il modo migliore per proteggere vostro figlio 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. Controlla, dalla cronologia il menu navigazione, 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 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 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 on- line da parte di cyberpredatori adulti: condividi con tuo figlio le procedure per navigare in sicurezza ed evitare on-line ed off-line brutti incontri. Confrontati con suo figlio su tutti questi rischi e se 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 salone o in una stanza accessibile a tutta la famiglia e non nella camera di tuo figlio ALMENO fino ai 16 anni.

Protocolli siglati con le forze dell’ordine e i servizi del territorio per la gestione condivisa dei casi. Non vi sono protocolli siglati ma ricorrenti forme di collaborazione nella prevenzione e contrasto del bullismo e del cyberbullismo da parte dell’Ente Locale e del Comando dei Carabinieri.

Siti utili

http://www.azzurro.it/it

www.generazioniconnesse.it

www.commissariatodips.it