



Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

Il seguente documento programmatico è volto a promuovere le competenze digitali ed un uso delle tecnologie costruttivo, critico e consapevole, sia da parte dei ragazzi e delle ragazze che della comunità educante.

L'E-policy, inoltre, è 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 visione educativa e la proposta formativa del Collegio S. Ignazio, 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.

L'E-policy è 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.

Obiettivo principale del presente documento è informare l'utenza per un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente. In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali .

I minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti.

Gli insegnanti hanno la responsabilità di guidare gli studenti nelle attività online a scuola e di indicare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa, per prevenire il verificarsi di situazioni potenzialmente pericolose.

Ruoli e responsabilità

Affinché l'E-policy sia davvero uno strumento operativo efficace per la scuola e tutta la comunità educante è necessario che ogni componente, secondo il proprio ruolo, s'impegno 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);
- ✚ 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 rete;
- ✚ 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.

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).

Definizione e disciplina delle Azioni Antibullismo

Condivisione e comunicazione dell'ePolicy 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.

Condividere e comunicare la politica di e-safety agli alunni

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

La linea di condotta della scuola in materia di sicurezza nell'utilizzo delle tecnologie digitali e di internet sarà discussa negli organi collegiali e comunicata formalmente a tutto il personale con il presente documento e altro materiale informativo anche sul sito web.

Per proteggere tutto il personale e gli alunni, Il **Collegio S. Ignazio** attuerà una linea di condotta di utilizzo accettabile, controllato e limitato alle esigenze didattiche essenziali.

Il personale docente sarà reso consapevole del fatto che il traffico in internet può essere monitorato e si potrà risalire al singolo utente registrato.

Un'adeguata informazione/formazione on-line del personale docente nell'uso sicuro e responsabile di internet, sia professionalmente che personalmente, sarà fornita a tutto il personale, anche attraverso il sito web della scuola.

Il sistema di filtraggio adottato e il monitoraggio sull'utilizzo delle TIC sarà supervisionato dall'Animatore digitale, che segnalerà al DSGA eventuali problemi che dovessero richiedere acquisti o interventi di tecnici;

L'Animatore digitale metterà in evidenza on-line utili strumenti che il personale potrà usare con gli alunni in classe. Questi strumenti varieranno a seconda dell'età e della capacità degli alunni. Tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è sanzionabile.

Condividere e comunicare la politica di e-safety ai genitori

L'attenzione dei genitori sulla sicurezza nell'uso delle tecnologie digitali e di internet sarà attirata nelle news o in altre aree del sito web della scuola;

Sarà incoraggiato un approccio di collaborazione nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione degli incontri scuola-famiglia, assembleari, collegiali e individuali. L'Animatore digitale fornirà ai genitori suggerimenti e indicazioni per l'uso sicuro delle tecnologie digitali e di internet anche a casa.

L'Animatore digitale e i docenti di classe forniranno ai genitori indirizzi sul web relativi a risorse utili per lo studio e a siti idonei ed educativi per gli alunni, sistemi di filtraggio e attività educative per il tempo libero.

Gestione delle infrazioni alla ePolicy

Le infrazioni all'E-policy saranno gestite dalla scuola 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, 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;
- 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. **Più bassa è l'età degli alunni 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 l’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;
- ✓ 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.

Integrazione dell'ePolicy con Regolamenti esistenti

Il Regolamento dell'Istituto Scolastico viene aggiornato con specifici riferimenti all'E-policy, così come anche il Patto di Corresponsabilità, in coerenza con le Linee Guida Miur e le indicazioni normative generali sui temi in oggetto.

La policy richiede l'integrazione con l'inserimento delle seguenti norme:

- ✓ Le apparecchiature presenti nella scuola sono un patrimonio comune, quindi, vanno utilizzate con il massimo rispetto.
- ✓ Le postazioni informatiche dell'istituto possono essere utilizzate esclusivamente per attività di insegnamento, funzionali all'insegnamento e di formazione del personale docente e non docente.
- ✓ In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile.
- ✓ In caso di malfunzionamento non risolvibile dal responsabile di laboratorio, il suddetto contatterà la segreteria e poi il tecnico.

Disposizioni sull'uso dei software

1. I software installati sono ad esclusivo uso didattico.
2. 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.
3. E' fatto divieto di usare software non conforme alle leggi sul copyright. E' 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.
4. E' 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

1. 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;

2. Internet non può essere usato per scopi vietati dalla legislazione vigente;

3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;

4. È vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza.

Norme finali

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.

UTILIZZO DEL TELEFONO CELLULARE E DEI VARI DISPOSITIVI ELETTRONICI DURANTE LE ATTIVITÀ SCOLASTICHE

Salvo casi del tutto eccezionali, i telefoni cellulari non devono essere portati a scuola e non devono comunque essere utilizzati durante l'orario scolastico. Se gli studenti verranno sorpresi ad usare il cellulare, lo stesso verrà temporaneamente requisito dai docenti che registreranno l'episodio sul registro di classe e – in collaborazione con il personale ausiliario e/o con la segreteria – convocheranno per le vie brevi i genitori interessati ai quali verrà riconsegnato il cellulare requisito. Avuto inoltre riguardo per il fatto che i moderni cellulari possono essere utilizzati anche per scattare foto (o effettuare riprese filmate) e per trasferirle, si informano i Sigg. genitori che eventi di questo tipo – se si concretizzano durante l'orario scolastico – si possono configurare anche come reati per i quali non si esclude la segnalazione ai competenti organi di Pubblica Sicurezza.

L'Istituzione Scolastica non ha e comunque non si assume alcuna responsabilità né relativamente all'uso improprio o pericoloso che gli studenti dovessero fare del cellulare (es.: inviare/ricevere messaggi a/da soggetti ignoti agli stessi genitori), né relativamente a smarrimenti e/o 'sparizioni di telefonini cellulari o di lettori mp3 o di hard/disk portatili o pen drive. In ogni caso, i genitori tengano conto che le comunicazioni urgenti ed improcrastinabili possono essere trasmesse ai loro figli durante l'orario scolastico rivolgendosi telefonicamente alle singole sedi scolastiche ovvero in Segreteria.

La scuola non pone alcun ostacolo all'utilizzo di cd/dvd rom o di hard - disk portatili come strumenti di lavoro e di studio. Ciò che a riguardo compete alle famiglie è il controllo periodico del contenuto di questi strumenti per evitare che qualche studente 'trasporti' a scuola immagini

/ testi / filmati per così dire ‘sconvenienti’, avendoli scaricati. Per impedire che le stesse postazioni dei laboratori scolastici possano essere furtivamente utilizzate per visitare siti volgari e pericolosi, la scuola si è da tempo dotata di un software di sicurezza che filtra gli accessi ad internet e protegge quindi i visitatori meno esperti. Oltre a questo sofisticato sistema di protezione che blocca l’accesso ai siti di cui si discorre, la scuola ovviamente mette in campo soprattutto la vigilante attenzione educativa di ogni singolo docente.

Monitoraggio dell’implementazione della ePolicy 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.

Piano di azioni del Collegio S. Ignazio

Azioni da svolgere entro un’annualità scolastica:

- ✓ Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i docenti dell’Istituto per la stesura finale dell’ePolicy.
- ✓ Organizzare incontri per la consultazione degli studenti/studentesse sui temi dell’ePolicy per cui si evidenzia la necessità di regolamentare azioni e comportamenti.
- ✓ Organizzare uno o più eventi o attività volti a presentare il progetto e consultare i genitori dell’Istituto per la stesura finale dell’ePolicy.

Formazione e curriculum

Curriculum 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 curriculum digitale.

COMPETENZA CHIAVE EUROPEA (Dalla Raccomandazione 2006/962/CE del 18 dicembre 2006 del Parlamento europeo e del Consiglio). Competenze digitali

<u>TRAGUARDI DI COMPETENZA</u> <i>(Dalle "Indicazioni Nazionali per il curriculum della scuola dell'infanzia e del primo ciclo di istruzione 2012". D.M. n. 254 del 16 novembre 2012.)</i>	COMPETENZE DI BASE	CONOSCENZE	ABILITÀ	VALUTAZIONE DEGLI APPRENDIMENTI
<u>SCUOLA DELL' INFANZIA</u>	Utilizzare le nuove tecnologie con la supervisione dell'insegnante.	<ul style="list-style-type: none"> ✓ Pc ✓ Mouse ✓ Tastiera ✓ Tablet 	Eseguire giochi al computer o alla LIM. Visionare immagini, opere artistiche, documentari	Con la supervisione dell'insegnante, conoscere l'utilizzo del computer per attività.
<u>SCUOLAPRIMARIA</u>	Usa le tecnologie in contesti comunicativi concreti per ricercare dati e informazioni e per interagire con soggetti diversi.	Utilizzare le più comuni Tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo, culturale e sociale in cui vengono applicate.	Procedure per la produzione di testi. Procedure di utilizzo di reti informatiche per ottenere dati, fare ricerche, comunicare.	Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini. Utilizzare materiali digitali per l'apprendimento. Utilizzare la rete per scopi di informazione, comunicazione, ricerca e svago.
<u>SCUOLA SECONDARIA</u>	Utilizzare le più comuni Tecnologie dell'informazione e della comunicazione, individuando le soluzioni potenzialmente utili ad un dato contesto applicativo, a partire dall'attività di studio. Essere consapevole delle potenzialità, dei limiti e dei rischi dell'uso delle tecnologie dell'informazione e della comunicazione, con particolare riferimento al contesto produttivo,	Utilizzare strumenti informatici e di comunicazione per elaborare dati, testi e immagini e produrre documenti in diverse situazioni. Utilizzare materiali digitali Per L'apprendimento Utilizzare il PC, periferiche e programmi Applicativi. Utilizzare la rete per scopi di informazione, comunicazione,	Utilizzare i mezzi informatici per redigere i testi delle ricerche, delle relazioni... Utilizzare power point per effettuare semplici presentazioni. Utilizzare la posta elettronica per corrispondere tra pari, con istituzioni, per relazionarsi con altre scuole anche straniere; Utilizzare Internet e i motori di ricerca per	Le applicazioni tecnologiche quotidiane e le relative modalità di funzionamento. Il sistema operativo e i più comuni software applicativi anche Open source Procedure per la produzione di testi, ipertesti, presentazioni. Procedure di

	culturale e sociale in cui vengono applicate.	ricerca e svago.	ricercare informazioni, con la supervisione dell'insegnante.	utilizzo di reti informatiche per ottenere dati, fare ricerche, comunicare.
--	---	------------------	--	---

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.

Gli insegnanti devono raggiungere un buon livello di formazione in merito all'utilizzo e all'integrazione delle TIC nella didattica. L'Istituto, attraverso il Collegio dei Docenti, riconosce e favorisce la partecipazione del personale ad iniziative promosse sia dalla scuola, dalle Reti di scuole, dall'Amministrazione, sia da quelle scelte liberamente dai docenti, purché coerenti con il piano di formazione. Fondamentale porre attenzione all'uso del TIC nella didattica: un loro utilizzo strutturato e integrato rende gli apprendimenti motivanti, coinvolgenti ed inclusivi e permette al docente di guidare studenti e studentesse nella fruizione dei contenuti online, sempre più importante anche in ambito lavorativo (lavoro di gruppo anche a distanza, confronto fra pari in modalità asincrona).

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.

I momenti di formazione e aggiornamento saranno pensati e creati a partire;

- ✓ dall'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica;
- ✓ dall'analisi del fabbisogno conoscitivo circa particolari argomenti che si sentono come più cogenti per i docenti e l'Istituto;
- ✓ dall'analisi delle richieste che provengono dagli studenti e dalle studentesse in modo, poi, da riutilizzarli nel loro lavoro di educatori (attraverso le modalità che il docente indica e ritiene più confacente alla classe) quanto appreso durante la formazione ricevuta.

Verrà elaborato un cronoprogramma che consideri il triennio scolastico, in un'ottica di vera e propria programmazione, con azioni specifiche:

- ✓ Analizzare il fabbisogno formativo degli insegnanti sull'uso sicuro della Rete;
- ✓ Monitorare le azioni svolte per mezzo di specifici momenti di valutazione;
- ✓ Organizzare incontri con professionisti della scuola o con esperti esterni, enti/associazioni, etc

Sarà predisposta un'area specifica sul www.collegiosignazio.it con materiali formativi per gli insegnanti.

Nella sezione, saranno messi a disposizione materiali per l'aggiornamento sull'utilizzo consapevole e sicuro di Internet, prevedendo possibilità e modalità di condivisione fra gli insegnanti. Sempre sul sito istituzionale della scuola.

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. Il collegio S. Ignazio garantisce la massima informazione alle famiglie di tutte le attività e iniziative intraprese sul tema delle tecnologie digitali, previste dall'ePolicy 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.

Verrà Aggiornato il "Patto di corresponsabilità" con specifici riferimenti all'uso delle tecnologie digitali e all'e Policy, per informare e rendere partecipi le famiglie sul percorso da intraprendere con il documento e il piano d'azione.

Il piano d'azioni formativo

- ✓ 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 incontri con esperti per i docenti sulle competenze digitali.
- ✓ 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.
- ✓ Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

Gestione della strumentazione ICT della e nella scuola.

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

Sono dati personali le informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, etc.

Fra questi, particolarmente importanti sono:

- ✓ i dati che permettono l'identificazione diretta di una persona, come i dati anagrafici (ad es. nome e cognome);
- ✓ i dati che permettono l'identificazione indiretta, come un numero di identificazione (ad es. il codice fiscale, l'indirizzo IP, il numero di targa);

- ✓ i dati rientranti in particolari categorie: si tratta dei dati cosiddetti sensibili, cioè quelli che rivelano l'origine razziale o etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale di una persona. Il Regolamento (UE) 2016/679 (articolo 9) ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale;
- ✓ i dati relativi a condanne penali e reati: si tratta dei dati cosiddetti giudiziari, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad es. i provvedimenti penali di condanna definitiva, la liberazione condizionale, il divieto o obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Il Regolamento (UE) 2016/679 (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

I soggetti sono:

- ✓ L'interessato, che è la persona fisica alla quale si riferiscono i dati personali (art. 4, paragrafo 1, punto 1), del Regolamento UE 2016/679);
- ✓ Il titolare, che è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico, privato o l'associazione che adotta le decisioni sugli scopi e sulle modalità del trattamento (art. 4, paragrafo 1, punto 7), del Regolamento UE 2016/679);
- ✓ Il responsabile, che è la persona fisica o giuridica alla quale il titolare richiede di eseguire per suo conto specifici e definiti compiti di gestione e controllo del trattamento dei dati (art. 4, paragrafo 1, punto 8), del Regolamento UE 2016/679). Il Regolamento medesimo ha introdotto la possibilità che un responsabile possa, a sua volta e secondo determinate condizioni, designare un altro soggetto c.d. sub-responsabile (art. 28, paragrafo 2).

Trattamento dei dati è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate a dati personali o insiemi di dati personali. Ad esempio: la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, par. 1, punto 2, del Regolamento (UE) 2016/679).

I soggetti che procedono al trattamento dei dati personali altrui devono adottare particolari misure per garantire il corretto e sicuro utilizzo dei dati.

Il Collegio S. Ignazio in conformità al al Regolamento UE 2016/679 deve:

Redigere e mantenere un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti. Valutare i rischi sulla privacy: (definita nel regolamento Data Protection Impact Assessment o PIA) relativamente ad alcune tipologie di trattamento dei dati sensibili. Le istituzioni scolastiche pubbliche e private possono trattare anche dati sensibili,

come ad esempio dati relativi alle origini razziali per favorire l'integrazione degli/le alunni/e, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli/le alunni/e, come i dati vaccinali con le Asl.

Analizzare il processo sulla raccolta/gestione del consenso: occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio, all'interno di modulistica o sul proprio sito web istituzionale. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice e chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, ma devono ad esempio adeguare tutta la modulistica al Regolamento UE 2016/679 e predisporre una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.

Adottare idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti:

- ✚ analisi del sito web istituzionale di riferimento con proposte volte a migliorare la sicurezza e la protezione dei dati trattati proposte in messa in sicurezza della intranet scolastica sulle reti Wi-fi installate;
- ✚ utilizzo di black list per la navigazione (sistemi di filtraggio dei contenuti);
- ✚ uso di un firewall hardware (componente hardware che, utilizzando un certo insieme di regole predefinite, permette di filtrare ed eventualmente bloccare tutto il traffico da e verso una qualsiasi rete di computer, lasciando passare solo tutto ciò che rispetta determinate regole);
- ✚ istituire corsi di formazione destinati ai responsabili, agli incaricati ed eventualmente ai sub incaricati del trattamento.

Accesso ad Internet

L'accesso a Internet è:

1. Diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale;
2. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale;
3. Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete;
4. L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e

applicazioni anche distribuite;

5. Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità;

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.

1. 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;
2. Internet non può essere usato per scopi vietati dalla legislazione vigente;
3. L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet;
4. E' vietato inserire sui pc connessi in rete programmi contenenti virus, scaricare software non autorizzati da internet, scaricare e installare software senza licenza. Norme finali 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.

Strumenti di comunicazione online

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

Il Nostro Istituto è dotato, attualmente, di strumenti di comunicazione esterna e interna:

Fra gli strumenti di comunicazione esterna troviamo il sito web della scuola, il registro elettronico e la posta elettronica. Fra gli strumenti di comunicazione interna troviamo i precedenti e i gruppi informali di whatsapp.

In riferimento all'uso degli strumenti di comunicazione online per la circolazione di informazioni e comunicazione interne è importante ricordare quello che si può definire "diritto alla disconnessione". L'art. 22 (Livelli, soggetti, materie di relazioni sindacali per la Sezione Scuola) del CCNL 2016/2018, infatti, fa riferimento ai criteri generali per l'utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione fra vita lavorativa e vita familiare.

È importante sottolineare però che per le chat informali fra colleghi, o fra docenti e genitori, non esiste una vera e propria regolamentazione, e per tale ragione è fondamentale, a partire dal buon senso e da una riflessione sulle peculiarità del mezzo, che si elaborino regole condivise sull'uso delle stesse:

- ✚ Mettere in chiaro fin dall'inizio, comprendere e rispettare sempre le finalità del gruppo, scrivendo e pubblicando solo contenuti pertinenti a tali finalità;
- ✚ Usare sempre un linguaggio adeguato e il più possibile chiaro e preciso (come già sottolineato la comunicazione online si presta spesso a non pochi fraintendimenti);
- ✚ Evitare di affrontare in chat argomenti troppo complessi e controversi (la comunicazione online in una chat di gruppo non è adatta per la gestione di problematiche di questo tipo, che certamente è più opportuno affrontare in presenza o in un Consiglio di classe);
- ✚ Evitare discussioni di questioni che coinvolgono due o pochi interlocutori, onde evitare di annoiare e disturbare gli altri componenti del gruppo;
- ✚ Non condividere file multimediali troppo pesanti;
- ✚ Evitare il più possibile di condividere foto di studenti in chat;
- ✚ Indirizzare solo domande precise e chiare, a cui si possano dare risposte altrettanto brevi e precise;
- ✚ Evitare messaggi troppo spezzettati, cercando il più possibile di essere brevi ed esaustivi allo stesso tempo.

Il registro elettronico. Permette di visionare:

- ✚ L'andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
- ✚ I risultati scolastici (voti, documenti di valutazione);
- ✚ Condivisione di materiale scolastico;
- ✚ eventi (agenda eventi);
- ✚ comunicazione varie (comunicazioni di classe, comunicazioni personali).

Strumentazione personale

I dispositivi tecnologici sono parte integrante della vita personale di ciascuno, compresa quella degli/le 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 il più ampio PNSD.

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").




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

I tablet e i pc personali possono essere integrati nel lavoro nelle classi quando ben progettato e calibrato per discipline e obiettivi formativi e didattici.

Rischi on line: conoscere, prevenire e rilevare

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.

Le azioni di sensibilizzazione riguarderanno:

- ✚ accrescere la consapevolezza nel gruppo target di riferimento circa un determinato tema/bisogno/problema che potrebbe presentarsi in quel gruppo;
- ✚ incoraggiare il gruppo a modificare i propri comportamenti rendendoli più funzionali;
- ✚ diffondere all'esterno del gruppo di riferimento e quindi tra l'opinione pubblica una certa consapevolezza rispetto all'argomento di interesse;
- ✚ facilitare il coinvolgimento di soggetti esterni in modo da mettere insieme diverse idee per lavorare ad un obiettivo comune;
- ✚ favorire la diffusione di informazioni e servizi disponibili all'utilità collettiva (promuovere la conoscenza dell'ePolicy nella comunità scolastica).

In sintesi, è opportuno tenere in considerazione i seguenti aspetti:

- ✚ spingere le persone a desiderare un cambiamento;
- ✚ porre in evidenza la possibilità di generare un cambiamento;
- ✚ individuare le azioni che consentono di produrre il cambiamento.

Se il problema della "sicurezza" è difficilmente riconducibile esclusivamente all'esistenza in sé di alcuni rischi, più o meno gravie insidiosi, appare chiaro come le migliori strategie di intervento siano di carattere prevalentemente preventivo.

Prevenzione Universale. Un programma di questo tipo parte dal presupposto che tutti gli studenti siano potenzialmente a rischio. Si tratta quindi di interventi diretti al grande pubblico o a un intero gruppo di una popolazione che non è stato identificato sulla base del rischio individuale.

Efficacia: trattandosi di programmi ad ampio raggio gli effetti di questi programmi possono essere modesti se confrontati con programmi che "trattano" un gruppo con un problema specifico. Tuttavia, questi interventi possono produrre cambiamenti in grandi popolazioni (ad es. si pensi ad un programma dedicato alle competenze emotive,

oppure alla cittadinanza digitale).

Prevenzione Selettiva. Un programma dedicato ad un gruppo di studenti in cui il rischio online è presente. In questo caso la presenza del rischio è stata individuata tramite precedenti indagini, segnalazioni fatte dalla scuola, oppure dalla conoscenza della presenza di fattori di rischio in quel determinato territorio. In questi casi gli interventi sono mirati e prevedono programmi formativi strutturati che hanno l'obiettivo di migliorare le competenze digitali e le strategie di problem solving. Può essere un valido programma se si osservano casi in cui la prevenzione universale non ha dato gli esiti previsti.

Prevenzione Indicata. Un programma di intervento sul caso specifico, è quindi pensato e strutturato per adattarsi agli/lle studenti/studentesse con l'obiettivo di ridurre i comportamenti problematici, oppure dare supporto alle vittime. Per la sua natura questo tipo di intervento si avvale di professionalità diverse perché spesso affronta problemi legati alla salute mentale del minore per cui è opportuno coinvolgere anche la famiglia del/lla ragazzo/a. La responsabilità dell'azione preventiva ed educativa chiama in campo diverse agenzie educative oltre alla scuola, come la famiglia, ma non solo (istituzioni, associazioni, società civile, etc.), ciascuna con un proprio compito nei confronti di bambini e bambine e di adolescenti. Tali agenzie sono chiamate a collaborare ad un progetto comune, nell'ambito di funzioni educative condivise. La necessità di questa collaborazione nasce, più o meno consapevolmente, dal riconoscimento sia da parte dei genitori che da parte degli insegnanti della rispettiva difficoltà a svolgere da soli la propria funzione formativa ed educativa.

POLITICHE DI PREVENZIONE CYBERBULLISMO

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 online 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;

Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.

È prevista la nomina 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).

Le caratteristiche del fenomeno

L'impatto: la diffusione di materiale tramite Internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online e continuare a diffondersi). Un contenuto offensivo e denigratorio online può, quindi, diventare virale e distruggere in alcuni casi la reputazione della vittima. Nelle situazioni più gravi, le vittime di cyberbullismo si trovano costrette a dover cambiare scuola o addirittura città, ma questo spesso non le aiuta. La Rete, si sa, è ovunque.

La convinzione dell'anonimato: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile. Sentendosi protetti dall'anonimato ci si sente liberi e più forti nel compiere atti denigratori, senza il timore di essere scoperti. È importante tenere bene a mente, però, che quello dell'anonimato è un "falso mito della Rete". Ogni nostra azione online è, infatti, rintracciabile e riconducibile a noi con gli strumenti opportuni o con l'intervento della Polizia Postale. L'anonimato del cyberbullo, inoltre, è anche uno dei fattori che stanno alla base del forte stress percepito dalla vittima, la quale molte volte non può dare né un nome e né un volto al proprio aggressore;

L'assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio. La vittima può essere raggiungibile anche a casa e vive nella costante percezione di non avere vie di fuga. Spegnerne il cellulare o il computer non basta, così come cancellare tutti i propri profili social. Il solo pensiero che eventuali contenuti denigratori continuino a diffondersi online è doloroso e si accompagna ad un senso costante di rabbia e impotenza.

L'assenza di limiti temporali: può avvenire a ogni ora del giorno e della notte.

L'indebolimento dell'empatia: esistono cellule chiamate neuroni specchio che ci permettono di "leggere" gli altri quando li abbiamo di fronte, capirli e di provare emozioni simile a quelle che loro provano, proprio come se fossimo di fronte ad uno specchio. Tale sensazione è data

dall'attivazione di una particolare area del cervello. Quando le interazioni avvengono prevalentemente online la funzione speciale di questi neuroni viene meno (mancando la presenza fondamentale dell'altro che è sostituito dal dispositivo). La riduzione di empatia che ne consegue può degenerare nei comportamenti noti messi in atto dai cyberbulli.

Il feedback non tangibile: il cyberbullo non vede in modo diretto le reazioni della vittima e, ancora una volta, ciò riduce fortemente l'empatia e il riconoscimento del danno provocato.

Per questo non è mai totalmente consapevole delle conseguenze delle proprie azioni. L'impossibilità di vedere con i propri occhi l'eventuale sofferenza e umiliazione provata dalla vittima fa sì che il tutto venga percepito come "uno scherzo" divertente a cui partecipare, di cui ridere o a cui essere indifferenti. Inoltre, il cyberbullismo non lascia segni fisici evidenti sulla vittima e si consuma in un contesto virtuale che spesso viene percepito dai ragazzi come non "reale", come un mondo ludico a sé stante.

È possibile suddividere gli atti di cyberbullismo in due grandi gruppi:

cyberbullismo diretto: il bullo utilizza strumenti di messaggistica istantanea che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei.

cyberbullismo indiretto: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

È molto importante sottolineare come il cyberbullismo non sia una problematica che riguarda unicamente vittima e cyberbullo. È un fenomeno sociale e di gruppo. Infatti, centrale è il ruolo delle agenzie educative e di socializzazione (formali e informali) più importanti per gli adolescenti: la famiglia, la scuola, i media, le tecnologie digitali e il gruppo dei pari.

Azioni di riconoscimento del cyberbullismo

Alcuni segnali generali che può manifestare la potenziale **vittima di cyber bullismo**

- ✚ Appare nervoso quando riceve un messaggio o una notifica;
- ✚ Sembra a disagio nell'andare a scuola o finge di essere malato (ha spesso mal di stomaco o mal di testa);
- ✚ Cambia comportamento ed atteggiamento in modo repentino;
- ✚ Mostra ritrosia nel dare informazioni su ciò che fa online;
- ✚ Soprattutto dopo essere stato online, mostra rabbia o si sente depressa;
- ✚ Inizia ad utilizzare sempre meno Pc e telefono (arrivando ad evitarli);
- ✚ Perde interesse per le attività familiari o per le attività extra-scolastiche che prima svolgeva;
- ✚ Il suo rendimento scolastico peggiora.

La normativa in materia

Il Parlamento italiano ha approvato il 18 maggio 2017 la Legge 71/2017, “Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo”, una legge a tutela dei minori per la prevenzione e il contrasto al cyberbullismo che prevede misure prevalentemente a carattere educativo/rieducativo. La legge pone al centro il ruolo dell’istituzione scolastica nella prevenzione e nella gestione del fenomeno e ogni Istituto scolastico dovrà provvedere ad individuare fra i docenti un referente con il compito di coordinare le iniziative di prevenzione e di contrasto del cyberbullismo. Questi aspetti vengono chiariti nel dettaglio dalle Linee di orientamento per la prevenzione e il contrasto del cyberbullismo.

Nella consapevolezza che le azioni efficaci siano quelle che ricorrono agli strumenti educativi, rieducativi e di mediazione del conflitto, esistono tuttavia responsabilità da conoscere, la possibilità di commettere reati o danni civili e specifici dispositivi giuridici.

Sempre la Legge 71/2017 introduce un provvedimento di carattere amministrativo per gli autori di atti di cyberbullismo, la procedura di ammonimento da parte del Questore: il minore autore può essere convocato dal Questore e ammonito se ritenuto responsabile delle azioni telematiche.

Più precisamente, la procedura di ammonimento prevista in materia di stalking (art. 612-bis c.p.), incasso di condotte di ingiuria (art. 594 c.p.), diffamazione (art. 595 c.p.), minaccia (art. 612 c.p.) e trattamento illecito di dati personali (art. 167 del codice della privacy) commessi mediante internet da minori ultraquattordicenni nei confronti di altro minore, se non c’è stata querela o non è stata presentata denuncia, è stata estesa al cyberbullismo e può essere impartita da parte del questore che convoca il minore, insieme ad almeno un genitore o a chi esercita la responsabilità genitoriale. Gli effetti dell’ammonimento cessano al compimento della maggiore età.

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

I ragazzi e le ragazze che fanno azioni di bullismo possono commettere reati. Secondo il codice penale italiano i comportamenti penalmente rilevanti in questi casi sono:

- percosse (art. 581)
- lesione personale (art. 582)
- ingiuria (art. 594)
- diffamazione (art. 595)
- violenza privata (art. 610)
- minaccia (art. 612)
- danneggiamento (art. 635).

RESPONSABILITA' DEL DOCENTE/EDUCATORE/GENITORE

La legge sancisce che “nessuno può essere punito per un atto preveduto dalla legge come reato, se al momento in cui l’ha commesso, non era imputabile”. Cosa si intende per “imputabilità”? Vuol dire avere la cosiddetta “capacità d’intendere e volere”. Dunque, per poter avviare un procedimento penale nei confronti di un minore è necessario: che abbia almeno compiuto 14 anni; che, comunque, anche se maggiore di 14 anni, fosse cosciente e volente al momento del comportamento, cioè in grado di intendere e volere (tale non sarebbe, per esempio, un ragazzo con degli handicap psichici). Le responsabilità per atti di bullismo e cyberbullismo compiute dal minorenne possono ricadere anche su:

- i genitori, perché devono educare adeguatamente e vigilare, in maniera adeguata all’età del figlio, cercando di correggerne comportamenti devianti. Questa responsabilità generale persiste anche per gli atti compiuti nei tempi di affidamento alla scuola (culpa in educando).
- gli insegnanti e la scuola: perché nei periodi in cui il minore viene affidato all’Istituzione scolastica il docente è responsabile della vigilanza sulle sue azioni e ha il dovere di impedire comportamenti dannosi verso gli altri/e ragazzi/.
- insegnanti e personale scolastico o verso Le strutture della scuola stessa. A pagare in primis sarà la scuola, che poi potrà rivalersi sul singolo insegnante. La responsabilità si estende anche a viaggi, gite scolastiche, manifestazioni sportive organizzate dalla scuola (culpa in vigilando).

Hate speech

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.

L’istituzione scolastica attua una serie di azioni finalizzate a:

- 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.

Attraverso:

- Informativa ai docenti, agli studenti, alle famiglie, al personale ATA

- Integrazione al Regolamento di Istituto
- Pubblicità

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 percorsi sul benessere Digitale attraverso:

- Conferenze di varia natura rivolto a genitori, insegnanti e studenti
- Formazione ai docenti
- Attivazione di supporto psicologico
- Azioni di sensibilizzazione

Adescamento online

Il grooming (dall'inglese "groom" - curare, prendersi cura) rappresenta una tecnica di manipolazione psicologica che gli adulti potenziali abusanti utilizzano per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata. Gli adulti interessati sessualmente a bambini/e e adolescenti utilizzano spesso anche gli strumenti messi a disposizione dalla Rete per entrare in contatto con loro.

I luoghi virtuali in cui si sviluppano più frequentemente tali dinamiche sono le chat, anche quelle interne ai giochi online, i social network in generale, le varie app di instant messaging (whatsapp, telegram etc.), i siti e le app di teen dating (siti di incontri per adolescenti). Un'eventuale relazione sessuale può avvenire, invece, attraverso webcam o live streaming e portare anche ad incontri dal vivo. In questi casi si parla di adescamento o grooming online.

Segnalazione e gestione dei casi Procedure dell'Istituto

Il personale docente del nostro Istituto quando ha il sospetto o la certezza che uno/a studente/essa possa essere vittima o responsabile di una situazione di cyberbullismo, sexting

o adescamento online ha a disposizione procedure definite e può fare riferimento a tutta la comunità scolastica.

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

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

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.

Il collegio S.Ignazio **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.

PROCEDURE DI SEGNALAZIONE

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 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.

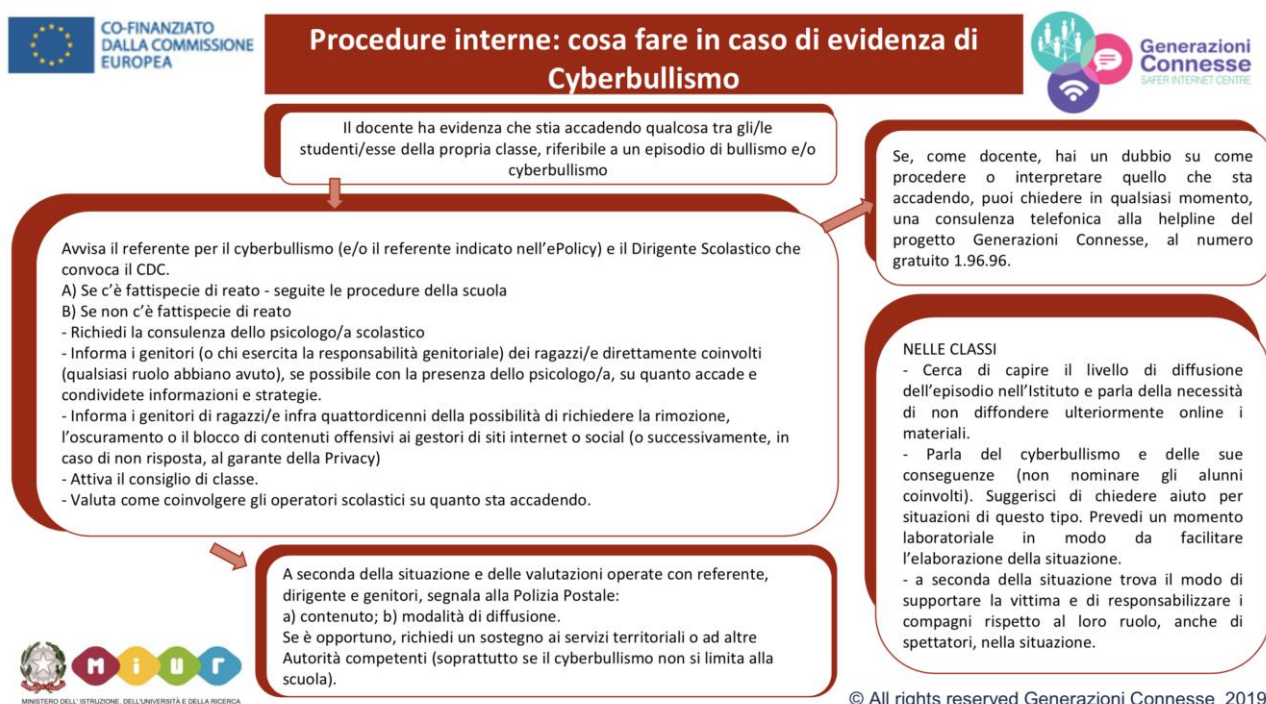
CASO EVIDENTE – Il docente ha evidenza certa che stia accadendo qualcosa tra gli/le studenti/esse della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo, sexting o adescamento online.

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

Strumenti a disposizione di studenti/esse

Per aiutare studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni, la scuola Prevede 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;
- docente referente per le segnalazioni.



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

