Ministero dell'Istruzione
ISTITUTO COMPRENSIVO
Via Vittorio Veneto, 72 – 24038 Sant'Omobono Terme (Bg)
tel. 035 851058 - www.icsantomobono.edu.it
e-mail: bgic87200p@istruzione.it - Cod. Fisc. n.: 95118250166

Politica della sicurezza online

E-SAFETY POLICY

Competenze digitali, uso critico e consapevole delle TIC, sicurezza online

La scuola elabora questo documento seguendo le indicazioni delle Linee di Orientamento per azioni di Prevenzione e di contrasto al bullismo e cyberbullismo (aprile 2015 e aggiornamenti ottobre 2017 e gennaio 2021) elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con Generazioni Connesse e il Safer Internet Center per l'Italia.

Approvato con Delibera Collegio dei Docenti in data 27 ottobre 2021

Indice

Introduzione 4

Azioni 5

Ruoli e Responsabilità 5

- Dirigente scolastico 6
- Direttore dei servizi generali e amministrativi 7
- Animatore digitale 7
- Amministratore digitale 7
- Referente Cyberbullismo 8
- Docente 9
- Personale ATA 10
- Alunni 11
- Genitori 12

Condivisione e comunicazione della policy 13

Gestione delle infrazioni della e-policy 13

- Potenziali infrazioni dei docenti 14
- Potenziali infrazioni degli studenti e delle studentesse 15

Integrazione della policy con Regolamenti esistenti 17

Formazione e Curricolo 17

Utilizzo del laboratorio di informatica e delle postazioni di lavoro 18

Prevenzione di situazioni a rischio cyberbullismo 19

L’osservazione e la rilevazione 20

Gestione e presa in carico delle situazioni a rischio 21

Procedura in caso di sospetto 21

Procedura in caso di evidenza 21

Indicazioni operative 22

Sitografia 23

Introduzione

Data la pervasività delle tecnologie nella quotidianità e la notevole familiarità degli alunni con gli strumenti informatici, la promozione dell'uso consapevole e critico delle TIC è da considerarsi un'opportunità ed una risorsa per la didattica.

La E-*safety Policy* è un documento programmatico elaborato dalla scuola volto a descrivere il proprio approccio alle tematiche legate alle competenze digitali, alla sicurezza online e ad un uso positivo delle tecnologie digitali nella didattica; le norme comportamentali e le procedure per l'utilizzo delle TIC (Tecnologie dell'Informazione e della Comunicazione) in ambiente scolastico; le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole delle tecnologie digitali.

La diffusione capillare di device che consentono il collegamento ad Internet offre molte opportunità, ma al contempo nasconde numerose insidie. La fruizione delle nuove tecnologie non può essere lasciata solo all'iniziativa personale e merita delle **azioni educative programmatiche per avviare e supportare i ragazzi nel loro uso critico e responsabile**. Gli alunni non devono essere lasciati soli nella gestione di strumenti, quali gli smartphone, ma supportati e sostenuti nel loro utilizzo civile e responsabile. Questo è alla base della prevenzione di azioni di cyberbullismo e di contrasto a qualsiasi forma di violenza psicologica legata all'uso delle chat o alla pubblicazione di foto e di video sui *social networks,* come già richiesto dalla Legge 107 del 2015, che ha introdotto, tra gli obiettivi formativi prioritari, lo sviluppo delle competenze digitali degli studenti, finalizzato anche a un utilizzo critico e consapevole dei social network e dei media, e declinato dal Piano Nazionale Scuola Digitale.

L'E-Safety comprende una serie di principi essenziali, la cui consultazione risulta necessaria quando si lavora online e si usano gli strumenti e le risorse della Rete. Ha come contenuti:

- ➢ la visione del fenomeno
- ➢ le norme comportamentali per tutta la Popolazione Scolastica
- ➢ le procedure di utilizzo delle TIC in ambiente scolastico
- ➢ le misure di prevenzione, rilevazione e gestione delle problematiche connesse all'uso delle Tic.

Azioni

Al fine di perseguire l'obiettivo di educare e sensibilizzare gli adolescenti, gli insegnanti e i genitori all'uso sicuro e consapevole delle TIC, l'E-Safety delinea le seguenti strategie:

- Avvio di percorsi di formazione per un uso consapevole delle TIC rivolti agli insegnanti nel corso dell'anno scolastico
- Coinvolgimento dei genitori come partner educativi nei percorsi di formazione che riguardano gli studenti
- Controllo dei dispositivi e delle reti laddove presenti da parte di tecnici incaricati
- Installazione e aggiornamento di firewall sull'accesso Internet (da parte di ditta specializzata)
- Presenza di un docente o di un adulto responsabile durante l'utilizzo di Internet, della piattaforma o di altre TIC
- Aggiornamento periodico del software antivirus e scansione dei pc in caso di sospetta presenza di virus da parte di tecnico incaricato/responsabile laboratorio

Ruoli e Responsabilità

Il personale dell'Istituto, i genitori e gli alunni si impegnano formalmente a seguire le leggi vigenti e a rispettare codesto documento.

Si fa esplicito divieto di caricare e utilizzare file o software non autorizzati e/o privi di licenza su tutti gli strumenti e i materiali informatici.

Chi utilizza Internet a scuola e in ambiente extrascolastico per lo svolgimento di attività di studio e ricerca, esplicitamente richieste dalla scuola, deve rispettare il seguente regolamento.

Nel caso di violazione di quanto stabilito, dopo aver considerato la gravità dei fatti, verranno presi provvedimenti come da Regolamento d'Istituto.

Non va dimenticato che la fruizione di Internet è tutelata e sanzionata da leggi dello Stato.

Ciascun utente connesso alla rete deve:

- rispettare il presente regolamento e la legislazione vigente;
- tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso;
- rispettare la cosiddetta *netiquette* (regole condivise che disciplinano il rapportarsi fra utenti della rete, wiki, siti, forum, mail e di qualsiasi altro tipo di comunicazione) cui si rimanda ai successivi paragrafi.

Di seguito vengono indicati i ruoli e gli incarichi dei diversi soggetti coinvolti.

Dirigente Scolastico

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

- verifica la legittimità di questo documento, secondo la normativa vigente in materia
- garantisce la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica
- promuove per tutti gli tutti gli insegnanti 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)
- garantisce l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line, l'applicazione di filtri di protezione per l'accesso ad internet per evitare la navigazione di siti inadeguati

- applica le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a infrazioni compiute dagli alunni nell'utilizzo delle TIC a scuola

- coordina linee di intervento per la gestione e la presa in carico dei casi di abuso o altre problematiche associate all'utilizzo di internet e delle tecnologie digitali.

Direttore dei Servizi Generali e Amministrativi

Il ruolo del Direttore dei Servizi Generali e Amministrativi include i seguenti compiti:

- assicura, 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;
- garantisce il funzionamento con le risorse economiche disponibili dei diversi canali di comunicazione della scuola (registro elettronico, account Istituto, 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, dell'Animatore digitale e del Referente Cyberbullismo nell'ambito dell'utilizzo delle tecnologie digitali e di internet.

Animatore digitale

Il ruolo dell'Animatore digitale include i seguenti compiti:

- stimola la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornisce informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- monitora e rileva le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola;
- propone l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola;
- coinvolge la comunità scolastica (alunni, genitori e altri attori del territorio) nelle attività e nei progetti attinenti la "scuola digitale".

Amministratore digitale

Il ruolo dell'Amministratore digitale include i seguenti compiti:

- assicura che gli utenti possano accedere alle Piattaforme Workspace for Education di Google e ArgoNext solo tramite password personali;
- cura l'aggiornamento del sito web della scuola per scopi istituzionali.

Referente Cyberbullismo

Il ruolo del Referente Cyberbullismo include i seguenti compiti:

- coordina azioni di sensibilizzazione per la diffusione di una cultura sull'uso consapevole delle TIC, in collaborazione con l'Animatore Digitale;

- offre strumenti per l'osservazione e la rilevazione dei segnali precursori di disagio/comportamenti a rischio relativamente all'uso non consapevole della rete;

- propone strumenti e azioni per la prevenzione di situazioni a rischio;

- propone procedure per la rilevazione delle problematiche derivanti da un uso non consapevole di internet;

- propone, in accordo col Dirigente, linee di intervento per la gestione e la presa in carico dei casi di abuso o altre problematiche associate all'utilizzo di internet e delle tecnologie digitali;

- riferisce al Dirigente Scolastico situazioni o problemi di particolare rilevanza su cui intervenire;

- raccoglie e diffonde buone pratiche educative, organizzative e azioni di monitoraggio, favorendo così l'elaborazione di un modello di e-policy d'istituto;

- collabora con gli organismi del territorio (Comuni, Forze di Polizia, associazioni…) per iniziative di prevenzione e contrasto del cyberbullismo ;

- cura la redazione e la revisione annuale della policy sulla base delle osservazioni ricevute da tutti i soggetti interessati; ne assicura la massima diffusione dentro la comunità scolastica in tutte le sue componenti (docenti, personale Ata, genitori e studenti).

Docente

Il docente nel libero esercizio della sua professionalità:

- illustra e ricorda ai propri alunni il regolamento d'Istituto riguardante l'utilizzo di internet, degli strumenti informatici e dei relativi software, i diritti inerenti il *copyright;*

- illustra agli alunni/e le regole di utilizzo delle TIC;

- si informa e si aggiorna sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet;

- offre indicazioni sul corretto utilizzo della rete;

- informa gli studenti sulla proprietà del software e sulla normativa riguardo il diritto d'autore, nonché sull'importanza di effettuare ricerche sul web e la relativa estrazione di documenti evitando il plagio o l'illecita diffusione di dati personali;

- propone agli alunni attività di ricerca e di informazione in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento;

- vigila che gli alunni non utilizzino le TIC senza l'autorizzazione e il controllo del docente, incorrendo in comportamenti scorretti e/o illeciti;

- segnala eventuali malfunzionamenti o danneggiamenti degli strumenti tecnologici al Responsabile del Plesso, che trasmetterà la segnalazione alla Segreteria della Scuola;

- segnala al Dirigente Scolastico e al Referente Scolastico del Bullismo e Cyberbullismo qualsiasi abuso rilevato a scuola, nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet;

- custodisce e non divulga le credenziali d’accesso degli account e delle reti Wi-fi;
- prende visione e sottoscrive la presente policy;
- non divulga dati anagrafici e sensibili di altri utenti adulti e/o degli alunni, contenuti nella documentazione in formato digitale cui ha accesso;
- lascia la postazione in ordine, sia nel laboratorio che in classe, avendo effettuato le corrette procedure per la disconnessione;
- non salva sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;
- usa i pc della scuola per scopi didattici e per le finalità connesse con il ruolo e la funzione docente;
- non utilizza file o software non autorizzati e/o privi di licenza.

Personale ATA

Il personale ATA:

- si informa per acquisire un’adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- prende visione e sottoscrive la presente policy;
- segnala qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'Animatore Digitale o al Referente Cyberbullismo per le opportune indagini / azioni / sanzioni;
- mantiene tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzate esclusivamente con sistemi ufficiali scolastici;
- custodisce e non divulga le credenziali d’accesso degli account.

Alunni

Le alunne/gli alunni sono responsabili per l'utilizzo corretto dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti da questa policy. In particolare:

- utilizzano le TIC su indicazioni del docente;
- accedono all'ambiente di lavoro in modo sicuro e consapevole in relazione al proprio grado di maturità e apprendimento;
- conoscono e capiscono l'importanza delle buone pratiche di sicurezza informatica a tutela dell'incolumità propria e altrui;
- devono essere istruiti rispetto alle 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;
- conoscono e rispettano le fondamentali norme relative alla privacy;
- devono acquisire consapevolezza sul significato e sulla gravità di atti di cyberbullismo;
- comprendono l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati e si informano circa il protocollo per tali segnalazioni;
- comunicano tempestivamente in caso di malfunzionamento e/o di contatto con informazioni immagini e/o applicazioni inappropriate;
- mantengono la configurazione del sistema operativo senza modificarlo;
- non utilizzano il proprio telefono cellulare e/o altri dispositivi elettronici e di intrattenimento (console portatili, mp3, ipod, ipad, notebook, fotocamera, videocamera) durante ogni attività scolastica, in tutti i locali della scuola, salvo specifiche deroghe autorizzate dal docente a integrazione dell'attività scolastica;
- tengono i propri dispositivi, se presenti, spenti e opportunamente custoditi in zaini o altro luogo.

Le comunicazioni tra alunni e famiglie, in caso di urgenza, vengono soddisfatte attraverso la Segreteria.

Genitori

Genitori e tutori svolgono un ruolo cruciale nel garantire che i loro figli comprendano la necessità di utilizzare i dispositivi Internet e mobili in modo appropriato. La scuola creerà occasioni per sensibilizzare i genitori su questo aspetto attraverso incontri con esperti, circolari, sito web e altre comunicazioni telematiche, informazioni su campagne di sicurezza promosse da altre istituzioni o su convegni dedicati a questo tema.
L'impegno da parte dei genitori è quello di fissare delle regole da far rispettare, anche in ambito domestico, primariamente assistendo i minori nel momento dell'utilizzo della rete e ponendo in atto tutti i sistemi di sicurezza.
I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di e-safety e a seguire le linee guida sull'uso appropriato di immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule; accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico; dispositivi personali dei loro figli nella scuola (dove ciò sia consentito).
Allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet, sia a casa che a scuola, tutti i genitori sono tenuti a prestare la massima attenzione ai principi e alle regole contenute nel presente documento.

In particolare:

- sostengono la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC;
- si informano circa le politiche d'uso di dispositivi mobili e device digitali;
- si istruiscono circa le politiche di utilizzo delle immagini e la gestione della privacy;
- sono consapevoli del significato e della gravità di atti di cyberbullismo;
- accompagnano il figlio nella gestione di device (smartphone, tablet, ...);
- stabiliscono i tempi di utilizzo di tali strumenti per il proprio figlio;

- stabiliscono le regole e le modalità per il controllo delle attività svolte dai propri figli sulla rete;

- in relazione all'uso delle TIC, verificano l'adeguatezza delle attività svolte dal ragazzo rispetto alla sua età e alla sua sensibilità.

Condivisione e comunicazione della policy

Per rendere efficace e fattiva la E-policy, l'Istituto s'impegna a prendere spunto da essa come base di partenza per azioni e iniziative riguardanti gli argomenti trattati nel documento.

La E-policy viene pubblicata sul sito della scuola nella sezione dedicata ai documenti. A tutta la comunità scolastica si chiede di prenderne visione. Per facilitare la presa in carico del documento si possono prevedere momenti di discussione collegiale sui contenuti, sulle pratiche indicate e su come inserire nel curricolo le tematiche di interesse della policy. Ogni modifica e miglioramento verrà opportunamente comunicata e condivisa.

Per la componente studentesca si potranno prevedere delle discussioni in classe sulla policy, sfruttando i primi giorni di scuola, con particolare riguardo al protocollo di accoglienza per le nuove classi prime.

Per i genitori si potranno organizzare incontri di sensibilizzazione sul tema della sicurezza informatica e sui comportamenti da monitorare o da evitare.

Gestione delle infrazioni della e-policy

Compito della Scuola è quello di favorire l'acquisizione delle competenze necessarie all'esercizio di una cittadinanza digitale consapevole. Responsabilizzare le alunne e gli alunni significa, quindi, mettere in atto interventi formativi, informativi e partecipativi. Tale principio è alla base dello Statuto delle studentesse e degli studenti che sottolinea la finalità educativa anche quando si rendano necessari provvedimenti disciplinari, comunque tesi a ripristinare comportamenti corretti all'interno dell'istituto *"attraverso attività di natura sociale e culturale ed in generale a vantaggio della comunità scolastica"* (LINEE DI ORIENTAMENTO per la prevenzione e il contrasto del cyberbullismo, ottobre 2017).

Le infrazioni alla policy possono essere rilevate da docenti/personale ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/personale ATA.

Qualora esse si configurino come **vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso.**

E' bene ricordare che, nel momento in cui un qualunque attore della comunità scolastica venga a conoscenza di un reato perseguibile d'ufficio, è fatto obbligo di denuncia (ex art. 331 del codice di procedura penale). L'omissione di denuncia costituisce reato (art. 361). I reati che, in ambiente scolastico, possono essere riferiti all'ambito digitale e commessi per via telematica sono tra gli altri:

- minaccia, in particolare, se la minaccia è grave; per tale reato si procede d'ufficio (art. 612 codice penale);
- induzione alla prostituzione minorile (art. 600bis);
- pedopornografia (art. 600 ter);
- corruzione di minorenne (art. 609 quinquies).

Nel caso in cui le infrazioni della e-policy violino norme previste dal Regolamento di Istituto, si procede secondo quanto previsto dal Regolamento stesso. Qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.

Potenziali infrazioni dei docenti

Il docente, nonché il personale scolastico (Dirigente, DSGA, Referente Cyberbullismo, Animatore digitale, assistente amministrativo), non deve pubblicare materiale scolastico sui siti o blog personali. La creazione di pagine online su social media relative a specifici progetti non deve contenere foto né dati sensibili che consentano di risalire alle generalità degli alunni.

Se le produzioni di fotografie o le effettuazioni di video riprese dovessero essere effettuate direttamente dai genitori, l'operazione esula dall'ambito di interesse del Codice sulla Privacy, in quanto il trattamento è effettuato da persona fisica per fini esclusivamente personali: ciò è peraltro garantito all'art 5 comma 3 del DL 30/06/2003 n 196. Lo stesso Garante, in comunicati stampa, ha ribadito che le riprese video raccolte

dai genitori, durante manifestazioni che riproducono momenti di vita scolastica, non violano la privacy in quanto niente hanno a che fare con la stessa: si tratta di immagini non destinate a diffusione, ma raccolte per fini personali e destinate ad un ambito familiare.

Si sottolinea che ai docenti è fatto divieto di:

- utilizzare le tecnologie d'uso comune con gli alunni per attività non connesse all'insegnamento o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiali non idonei;
- installare materiale protetto da copyright;
- collegarsi ad internet a scopi commerciali o di profitto personale e per attività illegali;
- trattare i dati personali comuni e/o sensibili degli alunni in modo non conforme ai principi della privacy;
- diffondere delle password assegnate oppure non dare adeguata custodia degli strumenti e degli accessi di cui possono approfittare terzi;
- eludere la vigilanza degli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti.

Tutto il personale scolastico è tenuto a collaborare e a fornire ogni informazione utile per le valutazioni del caso e l'avvio dei 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.

Potenziali infrazioni degli studenti/esse

Agli studenti/esse, in ambito scolastico, è fatto divieto di:

- 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;
- la condivisione di immagini intime o personali;

- il collegamento a siti web non indicati dai docenti;
- la comunicazione, incauta e senza permesso di un adulto, con sconosciuti su chat o blog;
- utilizzo del cellulare o altri dispositivi senza l'autorizzazione;
- riprendere o fotografare compagni, docenti, o luoghi scolastici.

Più gli alunni sono giovani 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.
Pertanto, in caso di infrazioni, presa visione del Regolamento di disciplina, si porranno in essere le seguenti procedure:

- **richiamo verbale da parte dell'insegnante;**
- **richiamo scritto;**
- **convocazione dei genitori da parte degli insegnanti;**
- **convocazione dei genitori da parte del Dirigente Scolastico.**

Se nonostante il divieto, gli alunni sono sorpresi ad usare il cellulare, lo stesso verrà requisito e riconsegnato come da Regolamento d'Istituto; l'insegnante provvederà a informare i genitori mediante una nota disciplinare sul Registro elettronico.
Se eventuali fotografie o video effettuati illecitamente durante l'orario scolastico si potranno ascrivere all'ambito del reato, la scuola chiederà l'intervento degli organi competenti di Pubblica Sicurezza.

L'Istituzione Scolastica, dopo aver messo in atto strategie per educare, prevenire, scoraggiare l'uso improprio del cellulare e altri dispositivi non previsti nell'ambito dell'attività scolastica, non si assume nessuna responsabilità, né relativamente all'uso improprio, né relativamente a smarrimenti o furti. Fermo restando che la scuola è un'istituzione educativa e che non è prevista, né possibile, né legittima, la perquisizione quotidiana di tutti gli alunni/e, le responsabilità che dovessero derivare dal verificarsi di eventi riconducibili all'uso non legittimo di device non autorizzati sono totalmente ascrivibili alle famiglie degli alunni coinvolti.

Integrazione della policy con Regolamenti esistenti

La presente policy è allegata in appendice al Regolamento di Istituto.

Formazione e Curricolo

Curricolo sulle competenze digitali per la componente studentesca

Le TIC e Internet sono un elemento essenziale nella vita del XXI secolo. La scuola ha il dovere di fornire alla componente studentesca l'accesso a questi strumenti come parte della loro esperienza di apprendimento e di far maturare in loro le competenze per una proficua cittadinanza digitale. L'uso delle TIC va inserito pertanto nel curricolo sia a livello disciplinare sia a livello interdisciplinare, peraltro come indicato anche nel curricolo di Educazione civica.

In particolare il curricolo dovrà essere strutturato per prevedere di:

- insegnare ciò che è accettabile nell'utilizzo di Internet e ciò che è vietato, fornendo strumenti per l'utilizzo efficace di Internet e la conoscenza delle conseguenze delle violazioni;
- mostrare come produrre, pubblicare e presentare contenuti digitali in modo appropriato, sia in ambienti privati sia per un pubblico più vasto;
- insegnare la valutazione dei contenuti Internet;
- impiegare materiali prelevati da Internet a scopi didattici conformemente al diritto d'autore;
- rendere alunne e alunni criticamente consapevoli dei materiali che si leggono sul web allo scopo di vagliare le informazioni prima di accettarne la fondatezza, la coerenza, le origini;
- insegnare le modalità di segnalazione di contenuti Internet sgradevoli o illegali.

Utilizzo del laboratorio di informatica e delle postazioni di lavoro

Le apparecchiature presenti nella scuola sono 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 dispositivi personali se non dopo opportuno controllo con sistema di antivirus aggiornato.

All'uscita dal laboratorio sarà cura di chi lo ha utilizzato lasciare il locale in ordine e le macchine spente correttamente.

In caso di malfunzionamento o guasto dei computer bisogna darne tempestiva segnalazione al responsabile del laboratorio.

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.

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.

Prevenzione di situazioni a rischio cyberbullismo

Le misure di prevenzione comprendono:

1. l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet . Nel curricolo si dovranno prevedere attività volte a lavorare su tre livelli: individuale, gruppo classe e istituzionale. La progettazione di unità didattiche specifiche deve essere pianificata a livello di dipartimenti disciplinari, garantendo un intervento su ogni classe, anche con docenti non titolari della classe. Si demanda ai settori disciplinari la scelta dei settori su cui focalizzare la formazione (a titolo di esempio, il dipartimento letterario si può soffermare in particolare sugli aspetti legati all'affettività, alla socializzazione e alla cittadinanza, quello tecnologico-scientifico-matematico sulle questioni tecniche e legate alla salute, quello di arte/musica sulla tutela del diritto d'autore, …).

2. Lo sviluppo di prassi e buone pratiche volte a far riflettere la comunità sull'uso corretto di internet e delle tecnologie digitali.

3. La collaborazione con enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica (le famiglie sono invitate a proporre tematiche di particolare interesse su cui la scuola focalizzerà il proprio intervento).

4. La presenza di uno sportello di ascolto, al quale la componente studentesca, i genitori e i docenti si possono rivolgere per avere consigli e sostegno psicologico anche relativamente alle tematiche del cyberbullismo.

5. La creazione di strumenti di osservazione rispetto ai segnali predittori di situazioni a rischio.

6. La progettazione di una procedura per la segnalazione delle situazioni a rischio.

7. La creazione di strumenti di segnalazione di situazioni di bullismo o cyberbullismo.

8. La progettazione di una procedura di gestione e presa in carico di situazioni critiche per giungere ad una soluzione.

L’osservazione e la rilevazione

E’ compito dell'intera comunità educante, l’osservazione e la rilevazione di situazioni critiche che potrebbero dare adito a casi di bullismo e cyberbullismo. A partire dalla corretta formazione e sensibilizzazione di tutti gli adulti coinvolti, docenti e personale ATA sono invitati a essere confidenti e custodi, diretti o indiretti, di ciò che le ragazze e i ragazzi vivono. Si raccomanda di evitare ogni atteggiamento accusatorio o intimidatorio per riuscire a ricevere, dai minori più fragili, segnalazioni e confidenze circa situazioni problematiche vissute.

Gli insegnanti sono chiamati a ricoprire un **ruolo privilegiato nell’individuazione e osservazione delle problematiche**, dei rischi, dei pericoli che bambine, bambini e adolescenti possono vivere e affrontare ogni giorno. Accorgersi tempestivamente di quanto accade e compiere azioni immediate di contrasto verso gli atti inopportuni - quando non illegali - diviene fondamentale per poter evitare conseguenze a lungo termine che possano pregiudicare il benessere e una crescita armonica dei soggetti coinvolti.

Sono da considerarsi **tipologie persecutorie qualificate come Bullismo**:

- la violenza fisica, psicologica o l’intimidazione del gruppo, specie se reiterata;
- l’intenzione di nuocere;
- l’isolamento della vittima.

Rientrano nel Cyberbullismo:

Flaming: Litigi *on line* nei quali si fa uso di un linguaggio violento e volgare.
Harassment: molestie attuate attraverso l’invio ripetuto di linguaggi offensivi.
Cyberstalking: invio ripetuto di messaggi che includono esplicite minacce fisiche, al punto che la vittima arriva a temere per la propria incolumità.
Denigrazione: pubblicazione all’interno di comunità virtuali, quali newsgroup, blog, forum di discussione, messaggistica immediata, siti internet… di pettegolezzi e commenti crudeli, calunniosi e denigratori.
Outing estorto: registrazione delle confidenze, raccolte all’interno di un ambiente privato, creando un clima di fiducia e poi inserite integralmente in un blog pubblico.
Impersonificazione: insinuazione all’interno dell’account di un’altra persona con l’obiettivo di inviare dal medesimo messaggi ingiuriosi che screditino la vittima.
Esclusione: estromissione intenzionale dall’attività on line.
Sexting: invio di messaggi via smartphone ed Internet, corredati da immagini a sfondo sessuale.

Procedura di gestione e presa in carico delle situazioni a rischio

La gestione dei casi rilevati va **differenziata a seconda della loro gravità**; fermo restando che è opportuna la condivisione a livello di Consiglio di Classe di ogni episodio rilevato, anche minimo, alcuni avvenimenti possono essere affrontati e risolti con la discussione collettiva in classe.

Altri casi ancora possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e come rimediare.

Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.

Per chiarire cosa fare in caso di sospetta situazione di bullismo/cyberbullismo, l'Istituto si è dotato di una procedura di gestione delle situazioni a rischio.

Procedura in caso di sospetto

Il docente SOSPETTA che stia accadendo qualcosa tra gli alunni/e della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo.

COSA FAI COME DOCENTE:

- condividi con i docenti del CdC e con il referente per il cyberbullismo
- valuta con lui/loro le possibili strategie di intervento
- valuta se è il caso di avvisare il consiglio di classe monitorando ciò che accade
- valuta se è il caso di avvisare il Dirigente Scolastico, anche in base al regolamento interno o a prassi consolidate
- sonda il clima di classe, ascoltando i ragazzi e monitorando ciò che accade (ma senza fare indagini o interrogatori)
- cerca di capire il livello di diffusione dell'episodio a livello di Istituto. (chiedere in classe, sondando tra gli studenti)

Procedura in caso di sospetto

Il docente HA EVIDENZA che stia accadendo qualcosa tra gli alunni/e della propria classe, riferibile a un episodio di bullismo e/o cyberbullismo.

COSA FAI COME DOCENTE

- Condividi con il referente per il cyberbullismo: valuta con lui/loro le possibili strategie di intervento.
- Avvisa il Dirigente Scolastico che convoca il CDC e/o CDI.

Se non c’è fattispecie di reato:

1. Richiedi la consulenza dello psicologo/a scolastico a supporto della gestione della situazione, in base alla gravità.

2. Informa i genitori (o chi esercita la responsabilità genitoriale) dei ragazzi/e direttamente coinvolti (qualsiasi ruolo abbiano avuto), se possibile con la presenza dello psicologo/a, su quanto accade e condividete informazioni e strategie.

3. Informa i genitori di ragazzi/e della possibilità di richiedere la rimozione, l’oscuramento o il blocco di contenuti offensivi ai gestori di siti internet o social (o successivamente, in caso di non risposta, al garante della Privacy).

4. A seconda della situazione e delle valutazioni operate con referente, dirigente e genitori, si attiverà la procedura per la segnalazione alla Polizia Postale.

Indicazioni operative

REATI/RISCHI	AZIONI
Adescamento online (Grooming)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet videogiochi, shopping o gambling online	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.

Esposizione a contenuti pornografici, violenti, razzisti	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. Verso la componente studentesca: inserimento nel curricolo di temi legati alla affidabilità delle fonti online, l'interculturalità e al rispetto delle diversità. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.
Sexting e pedopornografia	Verso i genitori: informazione circa le possibilità di attivare forme di controllo parentale della navigazione. Verso la componente studentesca: inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve, occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.
Violazione della privacy	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali.

Sitografia

Sito di Generazioni Connesse

https://www.generazioniconnesse.it/site/it/home-page/

Materiale per approfondimenti, moduli di segnalazione e sitografia disponibile nell'area web raggiungibile al link:

https://sites.google.com/didasweb.it/educare-ai-media/home

Tutorial per l'iscrizione alla piattaforma Generazioni Connesse:
https://screencast-o-matic.com/u/jnKK/piattaformagenerazioni

La scheda di prima segnalazione dei casi di bullismo e cyberbullismo

Nome del membro del team che compila lo screening:

Data:

Scuola:

1. Data della segnalazione del caso di bullismo:

2. La persona che ha segnalato il caso di bullismo era:

- ◯ La vittima
- ◯ Un compagno della vittima, nome
- ◯ Madre/ Padre della vittima, nome
- ◯ Insegnante, nome
- ◯ Altri:

3. Vittima, nome Classe:
   Altre vittime, nome Classe:
   Altre vittime, nome Classe:

4. Il bullo o i bulli
   Nome Classe:
   Nome Classe:
   Nome Classe:

5. Che tipo di prepotenze sono accadute? Dare esempi concreti degli episodi:

6. Quante volte sono successi gli episodi?

Valutazione approfondita dei casi di bullismo e vittimizzazione

Nome del membro del team che compila lo screening:

Data:

Scuola:

1. Data della segnalazione del caso di bullismo:

2. La persona che ha segnalato il caso di bullismo era:

- ◯ La vittima
- ◯ Un compagno della vittima, nome
- ◯ Madre/ Padre della vittima, nome
- ◯ Insegnante, nome
- ◯ Altri:

3. Nome e ruolo della persona della scuola che ha compilato il modulo del pre-screening:

4. Vittima, nome Classe:
   Altre vittime, nome Classe:
   Altre vittime, nome Classe:

5. Il bullo o i bulli
   Nome Classe:
   Nome Classe:
   Nome Classe:

6. Che tipo di prepotenze sono accadute? Dare esempi concreti degli episodi

7. In base alle informazioni raccolte, che tipo di bullismo è avvenuto?

- ☐ 1) è stato offeso, ridicolizzato e preso in giro in modo offensivo;
- ☐ 2) è stato ignorato completamente o escluso dal suo gruppo di amici;
- ☐ 3) è stato picchiato, ha ricevuto dei calci, o è stato spintonato;
- ☐ 4) sono stati messe in giro bugie/voci che hanno portato gli altri ad "odiarlo";
- ☐ 5) gli sono stati presi dei soldi o altri effetti personali (o sono stati rotti);
- ☐ 6) è stato minacciato o obbligato a fare certe cose che non voleva fare;
- ☐ 7) gli hanno dato dei brutti nomi, hanno fatto brutti commenti o gesti sulla sua etnia, colore della pelle, religione, orientamento sessuale o identità di genere;
- ☐ 8) ha subito delle offese o molestie sessuali, attraverso brutti nomi, gesti o att;
- ☐ 9) è stato escluso da chat di gruppo, da gruppi WhatsApp, o da gruppi online;
- ☐ 10) ha subito le prepotenze online tramite computer o smartphone con messaggi offensivi, post o fotografie su Facebook, su WhatsApp, Twitter, Myspace, Snapchat o tramite altri social media
- ☐ 11) ha subito appropriazione di informazioni personali e utilizzo sotto falsa identità della propria password, account (e-mail, Facebook…), rubrica del cellulare…

Altro:

8. Quante volte sono successi gli episodi di bullismo?

9. Quando è successo l'ultimo episodio di bullismo?

10. Da quanto tempo il bullismo va avanti?

11. Si sono verificati episodi anche negli anni precedenti?

12. Sofferenza della vittima:

La vittima presenta…	Non vero	In parte - qualche volta vero	Molto vero - spesso vero
Cambiamenti rispetto a come era prima	○	○	○
Ferite o dolori fisici non spiegabili	○	○	○
Paura di andare a scuola (non va volentieri)	○	○	○
Paura di prendere l'autobus – richiesta di essere accompagnato - richiesta di fare una strada diversa	○	○	○
Difficoltà relazionali con i compagni	○	○	○
Isolamento / rifiuto	○	○	○
Bassa autostima	○	○	○
Cambiamento nell'umore generale (è più triste, depressa, sola/ritirata)	○	○	○
Manifestazioni di disagio fisico-comportamentale (mal di testa, mal di pancia, non mangia, non dorme…)	○	○	○
Cambiamenti notati dalla famiglia	○	○	○
Impotenza e difficoltà a reagire	○	○	○

Gravità della situazione della vittima:

1	2	3
Presenza di tutte le risposte con livello 1	**Presenza di almeno una risposta con livello 2**	**Presenza di almeno una risposta con livello 3**
VERDE	**GIALLO**	**ROSSO**
○	○	○

Sintomatologia del bullo:

Il bullo presenta…	Non vero	In parte - qualche volta vero	Molto vero-spesso vero
Comportamenti di dominanza verso i pari	○	○	○
Comportamenti che prendono di mira i compagni più deboli	○	○	○
Uno status per cui gli altri hanno paura di lui/lei	○	○	○
Mancanza di paura/preoccupazione per le conseguenze delle proprie azioni	○	○	○
Assenza di sensi di colpa (se e rimproverato non dimostra sensi di colpa)	○	○	○
Comportamenti che creano pericolo per gli altri	○	○	○
Cambiamenti notati dalla famiglia	○	○	○

Gravità della situazione del bullo:

1	2	3
Presenza di tutte le risposte con livello 1	**Presenza di almeno una risposta con livello 2**	**Presenza di almeno una risposta con livello 3**
VERDE ○	**GIALLO** ○	**ROSSO** ○

Fenomenologia del bullismo: il gruppo e il contesto

13. Da quanti compagni è sostenuto il bullo?

14. Gli studenti che sostengono attivamente il bullo

Nome Classe

Nome Classe

Nome Classe

15. Quanti compagni supportano la vittima o potrebbero farlo?

16. Gli studenti che possono sostenere la vittima (nome, classe)

Nome Classe
Nome Classe
Nome Classe

16. Gli insegnanti sono intervenuti in qualche modo?

17. La famiglia o altri adulti hanno cercato di intervenire?

18. La famiglia ha chiesto aiuto?

DECISIONE

In base alle informazioni acquisite dalle diverse sezioni (gravità della sintomatologia della vittima, gravità della sintomatologia del bullo, caratteristiche del quadro contestuale del gruppo classe e della famiglia), si delinea come livello di priorità dell'intervento:

LIVELLO DI RISCHIO DI BULLISMO E DI VITTIMIZZAZIONE	LIVELLO SISTEMATICO DI BULLISMO E VITTIMIZZAZIONE	LIVELLO DI URGENZA DI BULLISMO E VITTIMIZZAZIONE
Codice verde	Codice giallo	Codice rosso
Situazione da monitorare con interventi preventivi nella classe	**Interventi indicati e strutturati a scuola e in sequenza coinvolgimento della rete se non ci sono risultati**	**Interventi di emergenza con supporto della rete**
○	○	○