

E-Safety Policy d'Istituto

(deliberato dal Collegio dei Docenti il 07.10.2020 e dal Consiglio d'Istituto il 30.10.2020)

■ INTRODUZIONE

Scopo della Policy

Il presente documento è da intendersi come cornice entro la quale devono essere inquadrare tutte le attività educativo-didattiche svolte da questo Istituto, allo scopo di favorire un uso consapevole della comunicazione, delle informazioni, delle immagini e dei dati digitali.

In particolare l'intento è promuovere la consapevolezza e l'atteggiamento critico da parte degli alunni riguardo le tecnologie digitali e la navigazione in rete e di assumere corrette norme comportamentali per favorire un corretto utilizzo delle stesse.

Ruoli e responsabilità

- Il Dirigente Scolastico:
 - ✓ promuove tutte le procedure di sicurezza (tra cui la sicurezza on line) fra i membri della comunità scolastica;
 - ✓ garantisce che tutti gli insegnanti ricevano una formazione adeguata per svolgere efficacemente la propria attività volta anche a promuovere la cultura dell'inclusione, del rispetto dell'altro/a e delle differenze, nonché un utilizzo positivo e responsabile delle *Tecnologie dell'Informazione e della Comunicazione* (TIC);
 - ✓ crea le condizioni per costruire un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on line;
 - ✓ gestisce eventuali casi di bullismo/cyberbullismo e definisce le procedure operative in collaborazione con il referente bullismo, i fiduciari di plesso e i docenti/coordinatori di classe.
- L'Animatore Digitale:
 - ✓ condivide e comunica la *Policy* all'intera comunità scolastica;
 - ✓ monitora l'implementazione della *Policy* e il suo aggiornamento.
- Il docente Referente Bullismo/Cyberbullismo/Legalità e i Fiduciari:
 - ✓ ricevono le segnalazioni;
 - ✓ collaborano alla gestione dei casi e all'attuazione delle procedure operative;
 - ✓ promuovono la cultura della legalità.
- Il Direttore dei Servizi generali e amministrativi (DSGA)
 - ✓ 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 ad un uso improprio o a dannosi attacchi esterni.
- Il Personale ATA è tenuto a:
 - ✓ avere adeguata consapevolezza circa le questioni di sicurezza informatica, la politica dell'Istituto e le relative buone pratiche;
 - ✓ prendere visione della presente *Policy*;
 - ✓ segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o figure preposte per le opportune indagini/azioni/ sanzioni;
 - ✓ mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici.
- I Docenti. Il ruolo del personale docente e di ogni figura educativa che lo affianca include:

- ✓ la segnalazione delle infrazioni alla *Policy*;
- ✓ l'informazione/aggiornamento sulle problematiche attinenti la sicurezza nell'utilizzo delle tecnologie digitali e della navigazione in rete, sulla politica di sicurezza adottata dalla scuola attraverso la conoscenza del *Regolamento*.

In particolare i docenti si impegnano a:

- ✓ contrastare un utilizzo scorretto e pericoloso delle TIC e di Internet da parte degli alunni;
 - ✓ verificare 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, fotocamere, etc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
 - ✓ nelle lezioni in cui è programmato l'utilizzo di Internet, guidare gli alunni a siti controllati e verificati come adatti per il loro uso e controllare che nelle ricerche su Internet siano trovati e trattati solo materiali idonei, cercando di ridurre al minimo gli inconvenienti;
 - ✓ 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;
 - ✓ attenersi alle indicazioni fornite dal piano d'azione, dalla *E-Safety Policy* e dal *Curricolo delle Competenze Digitali*.
- Gli Alunni. Il ruolo degli alunni include:
 - ✓ essere responsabili – a seconda del proprio grado di maturità e di apprendimento – riguardo all'utilizzo dei sistemi e delle tecnologie digitali in conformità con quanto richiesto dai docenti;
 - ✓ conoscere le possibilità della ricerca in rete 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;
 - ✓ usare le tecnologie della scuola solo in presenza di insegnanti o di figure deputate al controllo delle attività degli alunni;
 - ✓ adottare condotte rispettose degli altri anche quando si comunica in rete;
 - ✓ esprimere domande, difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.
 - I Genitori. Il ruolo dei genitori include:
 - ✓ sostenere la linea di condotta adottata dalla scuola 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 e della navigazione in rete.

■ FORMAZIONE E CURRICOLO

Curricolo sulle competenze digitali per gli studenti

È stato elaborato dal Collegio dei Docenti un *Curricolo delle Competenze civiche, sociali e di educazione civica* dove vengono evidenziate le competenze di cittadinanza digitale che gli alunni dovranno possedere al termine del primo ciclo. Lo stesso viene inserito nel PTOF dell'Istituto.

Formazione dei docenti sull'utilizzo e sull'integrazione delle TIC nella didattica

Nell'IC sono stati e saranno attivati:

- corsi di formazione interni sull'uso della piattaforma *GSuite for Education* e degli strumenti digitali più adeguati per la didattica nei tre ordini di scuola (Infanzia, Primaria, Secondaria I grado), sul coding e sul pensiero computazionale. Questi percorsi rientreranno nel *Piano di Formazione docenti* compreso nel PTOF;
- percorsi per docenti e studenti con la Polizia Postale e con esperti relatori al fine di diffondere le buone pratiche sull'uso consapevole della rete.

La partecipazione alla formazione sui rischi del WEB può essere estesa anche ai genitori e alla cittadinanza. Tali iniziative saranno periodicamente ripetute per raggiungere man mano tutti gli alunni. Si prevede anche di predisporre annualmente ad inizio anno scolastico un allineamento per i nuovi docenti sia sull'uso delle tecnologie sia sulle norme vigenti nell'Istituto.

■ GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE TIC DELLA SCUOLA

I docenti e gli alunni dell'Istituto hanno un account e un indirizzo mail d'Istituto (nome.cognome@icbadaloni.edu.it per i docenti e nome_cognome@icbadaloni.edu.it per gli alunni) utilizzati per lo svolgimento sia delle attività in DAD (didattica a distanza) e sia delle attività didattiche in presenza su apposita piattaforma digitale *GSuite* in uso nell'Istituto.

Si precisa che non è consentita la pubblicazione e la condivisione sui social network personali di materiali riferibili agli alunni (in particolare immagini di gite ed attività didattiche in cui gli alunni siano riconoscibili o identificabili).

Il materiale grafico o audio-visivo prodotto durante le attività didattiche e i progetti - all'interno del quale potrebbero essere stati ripresi anche gli alunni coinvolti nei percorsi proposti - potrà essere:

- caricato sulla piattaforma digitale in uso nella scuola ed essere quindi visionato dagli alunni sulla stessa accedendo con le proprie credenziali personali. Eccezionalmente potrà essere data la possibilità di scaricare tale materiale a condizione che i genitori/tutori/affidatari dei minori abbiano preventivamente firmato l'apposita liberatoria, assumendosi la responsabilità dell'eventuale uso di tale materiale;

- caricato su sito scolastico e visualizzato liberamente, a condizione che i genitori/tutori/affidatari dei minori abbiano preventivamente firmato l'apposita liberatoria.

Infine per l'uso dei devices personali (smartphone, tablet, etc.) si rimanda a quanto stabilito nel *Regolamento d'Istituto*.

Prevenzione uso scorretto della rete, gestione delle infrazioni, rilevazione e gestione dei casi di bullismo e cyberbullismo

• Prevenzione

✓ Rischi:

in questa *Policy* i rischi considerati sono quelli collegati all'uso scorretto della rete. I contenuti "pericolosi" per gli alunni messi in rete o scaricati dalla rete possono essere i seguenti:

1. contenuti afferenti alla privacy (foto personali, l'indirizzo di casa o il telefono, informazioni private proprie o di amici, foto o video pubblicati contro la propria volontà di eventi privati, etc.);
2. contenuti afferenti all'aggressività o alla violenza (messaggi minacciosi, commenti offensivi, pettegolezzi, informazioni false, foto o video imbarazzanti, virus, contenuti razzisti o che inneggiano al suicidio, immagini o video umilianti, insulti, videogiochi pensati per un pubblico adulto, etc.), partecipazione a giochi pericolosi quali *Blue Whale* e *Cutting*.
3. contenuti afferenti alla sessualità, quali messaggi molesti, conversazioni (chat o voce) che connotano una relazione intima e/o sessualizzata, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali (pedopornografia), etc..

✓ Azioni:

Le azioni previste di prevenzione attivate all'interno dell'Istituto nell'utilizzo delle TIC sono le seguenti:

1. informare e formare i docenti, i genitori, il personale ATA e gli alunni sui rischi che un uso non sicuro delle nuove tecnologie può favorire attraverso incontri con la Polizia Postale e workshop e convegni aperti a tutti;
2. aderire a progetti ministeriali e a occasioni che si presentano annualmente, anche coinvolgendo istituzioni locali, figure esperte, etc.;
3. all'inizio dell'anno scolastico fornire ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori (es.: liberatoria per la pubblicazione delle eventuali foto, immagini, testi e disegni relativi alla propria/o figlia/o);
4. non consentire l'utilizzo del cellulare personale dell'alunno per comunicare con i genitori, se non durante le uscite didattiche, in quanto per assolvere a ogni comunicazione urgente con i genitori o con chi ne fa le veci è sempre disponibile il telefono della scuola;
5. installare in tutti i plessi filtri e software che impediscono il collegamento ai siti web per adulti.

Gestione dei casi di violazione da parte degli studenti della Policy e della realizzazione di azioni di cyberbullismo (integrazione del Regolamento di Istituto)

INFRAZIONI	POSSIBILI SANZIONI
<ul style="list-style-type: none"> • L'uso di siti non-educativi durante le lezioni. • L'utilizzo non autorizzato di e-mail. • L'uso non autorizzato del telefono cellulare (o altre nuove tecnologie) durante le lezioni. • Uso di instant messaging/siti di social networking. 	<p>Fare riferimento all'insegnante di classe/Consiglio di Classe/ Dirigente Scolastico.</p> <ul style="list-style-type: none"> • Divieto di accesso a Internet per un periodo; • Requisizione del telefono fino a fine giornata scolastica; • Segnalazione disciplinare sul registro elettronico. • Contatto con i genitori.
<ul style="list-style-type: none"> • Uso di materiale offensivo. • Danneggiamento o distruzione deliberata dei dati altrui. • Violazione dell'altrui privacy. • Produzione di messaggi inappropriati, video o immagini su un sito di social networking o di instant messaging. 	<p>Fare riferimento all'insegnante della classe/ Consiglio di classe/Dirigente Scolastico.</p> <ul style="list-style-type: none"> • Divieto di accesso a Internet per un periodo. • Requisizione del telefono fino a fine giornata scolastica. • Contatto con i genitori. • Segnalazione disciplinare sul registro elettronico. • Ammonizione scritta con preavviso di sospensione. • Sospensione.
<ul style="list-style-type: none"> • Invio di e-mail o messaggi considerati molestia o bullismo. • Download o diffusione di qualsiasi materiale ritenuto offensivo, osceno, diffamatorio, razzista, omofobico o violento. • Trasmissione di materiale che viola i diritti d'autore di un'altra persona o infranga le condizioni della legge sulla protezione dei dati. • Discredito dell'immagine della scuola. 	<p>Fare riferimento all'insegnante della classe/ Consiglio di classe/Dirigente Scolastico/Consiglio d'Istituto/ Organo di garanzia/Autorità preposte.</p> <ul style="list-style-type: none"> • Divieto di accesso a Internet per un periodo. • Requisizione del telefono fino a fine giornata scolastica. • Contatto con i genitori • Segnalazione disciplinare sul registro elettronico. • Ammonizione scritta con preavviso di sospensione. • Sospensione • Contatto delle autorità competenti. <p>Altre possibili azioni di salvaguardia:</p> <ul style="list-style-type: none"> • Conservare le prove. • Informare i provider di servizi di posta elettronica del mittente. • Denunciare alle autorità competenti dove si sospetti la pedofilia o altre attività illegali.

■ APPROFONDIMENTI IN MERITO A CASI DI BULLISMO E CYBERBULLISMO

Rilevazione casi bullismo e cyberbullismo

In alcuni casi di bullismo o cyberbullismo gli alunni possono evidenziare particolari comportamenti/atteggiamenti quali segni di tristezza, ansia o di risentimento nei confronti di terzi.

Può accadere che riferiscano spontaneamente o su richiesta l'accaduto ai docenti o che siano proprio questi ad accorgersi di un'infrazione in corso. Nella prima circostanza potrebbe essere utile ricercare una "prova" di quanto riferito nella memoria degli strumenti tecnologici utilizzati a scuola o nei devices personali degli alunni, qualora questi ultimi siano disponibili a collaborare. Per il telefono cellulare ci si può assicurare che l'alunno vittima salvi nel suo telefono i messaggi, anche vocali, le immagini o i video incriminati e riferibili al mittente di cui pertanto si conserva il recapito.

Nella seconda circostanza, qualora ci si dovesse accorgere che l'alunno, usando il computer, si sta servendo di un servizio di messaggia istantanea o programma che permette di chattare in linea tramite testo, l'insegnante può copiare, incollare e stampare la conversazione. Per gli eventuali collegamenti non autorizzati a siti social network, video-hosting sites e altri websites ritenuti pericolosi, l'insegnante può conservare il link, stampare la pagina o salvare la schermata su documento word. Per le e-mail si può stampare la mail o conservare l'intero messaggio, compresa l'intestazione del mittente.

Conservare la prova è utile per far conoscere l'accaduto in base alla gravità ai genitori degli alunni, alla Dirigente scolastica e per le condotte criminose alla polizia.

Si ricorda a tale proposito che, in ogni caso, non è consentito l'utilizzo dei telefoni cellulari a scuola da parte degli alunni per tutto il tempo in cui sono affidati al personale dell'Istituto, fatta eccezione per quanto in precedenza asserito.

Anche i genitori possono segnalare alla scuola. La medesima può essere presentata attraverso un reclamo da parte dei genitori o può essere notata. In ogni caso il docente è autorizzato a controllare le strumentazioni della scuola e segnalare i contenuti inadeguati alla Dirigente scolastica. Per controllare l'uso del telefono cellulare di un alunno il docente si rivolge, invece, al genitore, nel caso in cui questi non fosse disponibile a collaborare.

Segnalazione

Sono previsti due tipi di segnalazione: interna ed esterna.

I docenti informeranno in prima battuta la Dirigente scolastica, con cui si valuteranno le situazioni caso per caso. Qualora non si disponga di prove, ma solo delle testimonianze dell'alunna/o, anche se riferite a fatti accaduti al di fuori del contesto scolastico, le notizie raccolte possono essere, a seconda dei casi, comunicate ai genitori e per fatti rilevanti e azioni criminose, anche alla Polizia. In particolare la segnalazione può essere fatta a entrambe le famiglie, se oltre alla vittima anche l'autore della condotta negativa è un altro alunno.

Gestione dei casi di bullismo cyberbullismo

Nell' I.C. "N. Badaloni" viene individuata una figura di riferimento quale *Referente per la prevenzione e il contrasto per il bullismo e il cyberbullismo e per la promozione della cultura della legalità*. Si sceglie prioritariamente un docente della Scuola Secondaria I grado, poiché in questa fascia d'età l'esposizione alla rete aumenta notevolmente.

La denuncia all'autorità giudiziaria o agli organi di Polizia deve essere fatta dalla Dirigente scolastica, quale legale rappresentante dell'Istituto, e costituisce il passo necessario per avviare un intervento di tutela a favore della vittima e attivare un procedimento penale nei confronti del presunto colpevole.

La scuola, quale agenzia educativa, assicura la sua collaborazione con le famiglie e le figure istituzionali e professionali coinvolte nella gestione dei casi; difatti compito della scuola non è solo quello di rilevare e denunciare quanto piuttosto prevenire l'abuso attraverso lo scambio di informazioni, la promozione di progetti, prassi operative e di occasioni di confronto e di dialogo.

Possibili azioni di contenimento

Le azioni di contenimento degli incidenti previste per contrastare l'uso incauto del web possono essere le seguenti:

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

Condivisione e comunicazione della *Policy* all'intera comunità scolastica

Questa *Policy* si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici della scuola. In particolare essa viene redatta per regolare il comportamento degli alunni dentro le aule scolastiche e per sensibilizzarli all'adozione di buone pratiche quando sono fuori dalla scuola e autorizza il personale docente a irrogare sanzioni disciplinari solo per comportamenti inappropriati avvenuti all'interno dell'istituzione scolastica o utilizzando la piattaforma d'Istituto *GSuite*.

La *Policy* sarà comunicata al personale, agli alunni, alla comunità nei seguenti modi:

- condivisione in sede di Collegio dei Docenti e inserimento nel PTOF;
- pubblicazione della E-Safety Policy quale allegato al *Regolamento d'Istituto* sul sito della scuola;
- comunicazione a genitori e alunni all'inizio dell'anno scolastico e nelle attività di orientamento;
- informativa agli studenti sull'uso responsabile della rete in modo tale che possano sviluppare "comportamenti sicuri";
- informativa al personale, agli alunni ed ai genitori su come segnalare azioni di bullismo o cyberbullismo.

Monitoraggio dell'implementazione della *Policy* e suo aggiornamento.

La *E-Safety Policy* sarà riesaminata annualmente e tutte le volte in cui si verificassero aggiornamenti normativi o cambiamenti riguardanti le tecnologie in uso all'interno della scuola.