ISTITUTO COMPRENSIVO STATALE "Emilio Alessandrini"

Via Bramante, 5 – 20090 Cesano Boscone (MI)
Tel. 02 45 01300 - codice univoco: MIIC8ES004
e-mail: miic8es004@istruzione.it miic8es004@pec.istruzione.it
URL: www.icsalessandrinicesanob.edu.it

Documento di E-Safety Policy

Sommario

1. Introduzione

1.1. Scopo della Policy.

La Policy di e-safety è un documento autoprodotto dalla scuola, sulla base dell'indice messo a disposizione da Generazioni Connesse, sito del progetto Safer Internet Center per l'Italia, volto a descrivere le norme comportamentali e le procedure per l'utilizzo delle *Tecnologie dell'informazione e della comunicazione* (TIC), le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.

Grazie a un percorso guidato e al materiale di supporto messo a disposizione sul sito del progetto www.generazioniconnesse.it, si definiscono qui le misure che l'Istituto intende adottare:

a) per la promozione dell'utilizzo delle ICT nella didattica;
b) per la prevenzione, ovvero le azioni finalizzate alla prevenzione di fenomeni legati ai rischi delle tecnologie digitali;
c) per la segnalazione dei casi, ovvero le disposizioni semplici su come segnalare i casi nella scuola;
d) per la gestione dei casi, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti che sono stati vittime o spettatori attivi e/o passivi di quanto avvenuto.

Occorre, inoltre, premettere che le attività di promozione all'utilizzo delle tecnologie digitali nella didattica costituiscono un tema centrale per l'attuazione del Piano Nazionale Scuola Digitale e sono previste nel Piano Triennale dell'Offerta Formativa, in particolare nel progetto predisposto dall'animatore digitale, come previsto dal Miur, e quindi non saranno trattate in questa policy. L'indirizzo che qui viene dato è che la prevenzione e la gestione dei casi di scorretto utilizzo delle tecnologie sono efficaci, solo se strettamente legate ad un loro uso quotidiano e consapevole.

1.2. Ruoli e responsabilità (che cosa ci si aspetta da tutti gli attori della ComunitàScolastica)

Nell'ambito di questa policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

1) Dirigente scolastico:

- garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- garantire ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ICT) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- seguire le procedure previste dalle norme in caso di reclami o attribuzioni di responsabilità al personale scolastico in merito a incidenti occorsi agli alunni durante l'utilizzo delle TIC a scuola.

2) Animatore digitale e Team digitale come da PNSD:

- *Formazione interna* - stimolare la formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di laboratori formativi, favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative, come ad esempio quelle organizzate attraverso gli snodi formativi;
- *Coinvolgimento della comunità scolastica* - favorire la partecipazione e stimolare il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, anche attraverso momenti formativi aperti alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa;
- *Creazione di soluzioni innovative* - individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; adozione di metodologie comuni; informazione su innovazioni esistenti in altre scuole; laboratorio di coding per tutti gli studenti), coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure.

3) Direttore dei Servizi Generali e Amministrativi:

- assicurare, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione richiesti affinché la dotazione tecnologica dell'Istituto sia funzionante, controllando al contempo che le norme di sicurezza vengano rispettate;
- facilitare la trasmissione di comunicazioni relative alle tecnologie digitali tra le varie componenti della scuola (Dirigente scolastico, Animatore digitale, docenti e famiglie degli alunni);
- curare la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti, provvedendo all'intervento del personale tecnico di assistenza.

4) Docenti:

- provvedere personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri:lotta al cyberbullismo);
- sviluppare le competenze digitali degli alunni e fare così in modo che conoscano eseguano le norme di sicurezza nell'utilizzo del web e utilizzino correttamente le tecnologie digitali sia a scuola sia nelle attività didattiche extracurricolari;
- segnalare al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni.
- segnalare prontamente alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabilire comuni linee di intervento educativo per affrontarle;

5) Alunni:

- ascoltare e seguire le indicazioni fornite dai docenti per un uso corretto e responsabile delle tecnologie digitali, cercando di essere il più possibile responsabili, attuando le regole di e-safety, per evitare situazioni di rischio;
- 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;
- adottare comportamenti rispettosi e non esporsi a rischi di violazione di privacy quando si comunica in rete;

- chiedere l'intervento dell'insegnante e/o dei genitori qualora insorgano domande o richieste di aiuto nell'utilizzo delle tecnologie didattiche o di internet per lo svolgimento dei compiti assegnati.

6) Genitori:

- contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete, dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- seguire l'uso che i propri figli fanno delle TIC nello svolgimento dei compiti a casa, controllando che tale utilizzo avvenga nel rispetto delle norme di sicurezza;
- agire in modo concorde con i docenti nell'adottare linee di intervento in relazione ai problemi derivanti da un uso non corretto e responsabile delle tecnologie digitali e di internet.

1.3. Condivisione e comunicazione della Policy all'intera comunità scolastica.

La E-safety Policy coinvolge tutti i membri dell'Istituto scolastico compreso il personale, gli studenti, i genitori e gli utenti della comunità che ne hanno accesso. Pertanto è necessaria la condivisione e la comunicazione della Policy a tutti gli attori della comunità scolastica.

a) Condivisione e comunicazione della Policy agli alunni:

- All'inizio dell'anno, in occasione della illustrazione del regolamento d'istituto agli alunni da parte dei docenti, verrà presentata questa policy, insieme ai regolamenti correlati;
- Nel corso dell'anno saranno dedicate da ciascun docente alcune lezioni alle buone pratiche per un utilizzo sicuro del digitale, con specifico riferimento ai rischi della rete e alla lotta al cyber bullismo (educazione civica).

b) Condivisione e comunicazione della Policy al personale:

- Le norme adottate dalla scuola in materia di sicurezza nell'utilizzo del digitale saranno discusse negli organi collegiali (collegio docenti, consigli di classe) e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito web della scuola.

- Il personale della scuola riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito web della scuola.

c) Condivisione e comunicazione della Policy ai genitori:

- Le famiglie saranno informate in merito alla linea di condotta adottata dalla scuola per un uso sicuro e responsabile delle tecnologie digitali e di internet attraverso la condivisione del presente documento e di materiali informativi specifici sul sito web della scuola.
- Al fine di sensibilizzare le famiglie sui temi dell'uso delle ICT saranno eventualmente organizzati dalla scuola incontri informativi, durante i quali si farà riferimento alla presente policy.

1.4. Gestione delle infrazioni alla Policy.

In relazione a quanto specificato in questo documento (e in modo particolare nella definizione dei ruoli del capitolo 1.2 e nelle regole descritte nei capitoli 3, 4 e 5), tutte le infrazioni alla presente Policy andranno tempestivamente segnalate al Dirigente Scolastico, che avrà cura di convocare le parti interessate onde valutare le possibili azioni da intraprendere in relazione alla gravità dell'infrazione e, nel caso degli alunni, anche alla loro età. Quanto qui di seguito descritto è poi meglio dettagliato nelle procedure allegate.

1) Infrazioni degli alunni.

È bene che i docenti introducano, preventivamente, attività laboratoriali miranti a sviluppare nei loro alunni una sempre maggiore consapevolezza dei rischi legati a un uso imprudente e improprio del web e che forniscano loro, ogni qualvolta avvenga un'infrazione alle regole stabilite, gli strumenti per affrontare le conseguenze dei loro errori.

I provvedimenti disciplinari da adottare da parte del consiglio di classe nei confronti dell'alunno che ha commesso un'infrazione alla policy (in proporzione sia all'età dello studente sia alla gravità dell'infrazione commessa) saranno i seguenti:

- richiamo verbale;
- sanzioni estemporanee commisurate alla gravità della violazione commessa (assegnazione di attività aggiuntive da svolgere a casa su temi di Cittadinanza e Costituzione; divieto temporaneo di prendere parte alla ricreazione e simili);

- nota informativa sul diario ai genitori;
- convocazione dei genitori per un colloquio con l'insegnante;
- convocazione dei genitori per un colloquio con il Dirigente Scolastico.

2) Infrazioni del personale scolastico.

Le infrazioni alla policy da parte del personale scolastico possono riguardare sia la mancata osservanza delle regole qui descritte sulla gestione della strumentazione, sia la mancata sorveglianza e pronto intervento nel caso di infrazione da parte degli alunni.

Nel primo caso la gravità si valuta sull'esposizione al rischio procurata agli alunni, nel secondo caso sul danno per la non tempestiva attivazione delle azioni qui indicate.

La gestione delle infrazioni in quest'ambito ricade nella disciplina contrattuale.

3) Infrazioni dei genitori.

Compito fondamentale dei genitori è supportare gli insegnanti e il personale scolastico nel riconoscimento e nella costruzione di azioni di contrasto efficaci ai principali rischi rappresentati dalla navigazione in internet di utenti molto giovani e spesso poco accorti.

Nel caso di mancanze da parte dei genitori si prevedono interventi per rafforzare il Patto di corresponsabilità scuola-famiglia.

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

Il monitoraggio dell'implementazione della Policy avverrà:

- alla fine di ogni anno scolastico, contestualmente al Rapporto di Autovalutazione e sulla base dei casi problematici riscontrati e della loro gestione;
- all'inizio di ogni anno scolastico, contestualmente alla revisione del PTOF, a cura del Dirigente scolastico, dell'Animatore digitale e della Funzione strumentale PTOF, anche attraverso la somministrazione ad alunni e docenti di questionari atti a verificare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

1.6. Integrazione della Policy con Regolamenti esistenti.

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti, che specificano il contesto di attuazione delle politiche dell'Istituto Comprensivo per un uso efficace e consapevole del digitale nella didattica:

- PTOF, incluso il piano per l'attuazione del PNSD;

- Regolamento interno d'Istituto;
- Protocollo di azione contro bullismo e cyberbullismo (allegato);
- Regolamento sull'uso dei cellulari (cfr. regolamento d'istituto);
- Regolamento per l'utilizzo dei laboratori fisici e mobili di informatica (parte integrante del presente documento).

2. Formazione e Curricolo

2.1. Curricolo sulle competenze digitali per gli studenti.

L'istituto ha un Curricolo sulle competenze digitali, stilato dall'Animatore Digitale sulla base delle indicazioni contenute nel PNSD (azione 14), in cui si individuano alcuni *framework* di riferimento per la definizione e lo sviluppo delle competenze digitali, come DigCompEdu (*quadro di riferimento europeo sulle competenze digitali dei docenti e dei formatori*) che individua una lista di 21 competenze descritte per conoscenze, abilità e atteggiamenti, comprese in 5 aree: Informazione, Comunicazione, Creazione di contenuti, Sicurezza e Problem solving. Tali framework sono quindi utili per identificare le competenze specifiche richieste, e in stretto contatto con la Information Literacy.

Nella definizione del curricolo si farà anche riferimento al modello sviluppato dal team di lavoro del prof. Antonio Calvani (centro Studi Erickson) per il ***Digital Competence Assessment*** e che qui si riporta per comodità di lettura; nella colonna di destra sono indicate le abilità richieste per ciascuna sfera considerata:

Dimensione tecnologica	a) riconoscere le criticità tecnologiche e le interfacce; b) selezionare la tecnologia adeguata per ciascun compito; c) operare logicamente; d) rappresentare processi simbolici; e) distinguere tra reale e virtuale.
Dimensione cognitive o *information literacy*	a) saper trattare (sintetizzare, rappresentare,analizzare) i testi, i dati, le tabelle e i grafici; b) saper valutare la pertinenza; dell'informazione e la sua affidabilità:
Dimensione etica	a) conoscere i concetti di tutela della privacy;

	b) rispettare i diritti intellettuali dei materiali reperiti in Internet e l'immagine degli altri (la lotta al cyberbullismo è un obiettivo importante di questa dimensione); c) comprendere il dislivello sociale e tecnologico che può esistere tra paesi, persone, generazioni, e il problema dell'accessibilità.
Obiettivo comune alle tre dimensioni	Saper comprendere il potenziale delle tecnologie; Di *networking* per costruire una conoscenza collaborativa.

2.2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica, sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

Le attività di formazione si svolgeranno su più livelli:

- formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodi formativi;
- formazione specifica di Istituto, legata alle esigenze formative rilevate ad inizio d'anno a cura dell'Animatore Digitale;
- attivazione e comunicazione di iniziative di formazione, in particolare rivolte allo sviluppo del pensiero computazionale attraverso il Coding;
- formazione e comunicazione di tutto il personale in materia di sicurezza on-line attraverso corsi di formazione e/o aggiornamento;
- adesione a progetti, come previsto nel PTOF, per prevenire e combattere forme di disagio giovanile quali bullismo e cyber bullismo;
- Incontro con forze dell'ordine per educare i ragazzi all'uso consapevole dei social network.

2.3. Sensibilizzazione delle famiglie

La scuola darà ampia diffusione, tramite pubblicazione sul sito, del presente documento di policy per consentire alle famiglie una piena conoscenza del regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e favorire un'attiva collaborazione tra la scuola e le famiglie sui temi della prevenzione dei rischi connessi a un uso inappropriato del digitale.

La scuola ha attivato uno sportello d'ascolto a disposizione degli alunni, delle famiglie e dei docenti per agevolare la segnalazione di problematiche emotive e relazionali, anche afferenti ad episodi di cyber-bullismo.

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola

3.1. Accesso a internet: filtri, antivirus e sulla navigazione

L'Istituto è costituito da più plessi tutti dotati di una discreta dotazione tecnologica. Nel plesso di Scuola Secondaria di Primo Grado "Alessandrini" in tutte le aule è presente la Lavagna Interattiva Multimediale con relativo computer portatile custodito in una aula blindata, due carrelli PC (laboratori mobili) e piccoli ambienti (sala docenti e aulette sostegno) con postazioni PC a disposizione del personale.

La connessione ad Internet è assicurata da una rete LAN e rete Wi-Fi scolastica, protette da password che consentono al personale di navigare in sicurezza.

L'accesso a internet è possibile, anche in tutti i plessi della scuola primaria dove in tutte le aule è presente la LIM.

Le impostazioni sono definite e mantenute dall'Animatore digitale in sinergia con il responsabile tecnico, ed è in carico a ciascun docente la segnalazione di malfunzionamenti e disservizi.

I docenti hanno piena autonomia nel collegamento ai siti web nelle postazioni a loro riservate.

3.2. Gestione accessi (password, backup, ecc.).

Nei computer presenti nelle aule e nei laboratori sono previsti tre profili di accesso con password relative:

- amministratore;
- docente;
- studente (libero accesso)

Non è previsto un backup automatico su server e non è al momento attiva una politica di backup.

3.3. E-mail.

È stato fornito dalla scuola un account di posta elettronica istituzionale. Le credenziali sono in possesso del personale.

I docenti utilizzano per scopi didattici sia il proprio account istituzionale prestando attenzione a:

- spam: e-mail, messaggi istantanei indesiderati

- Phishing: truffa effettuata su Internet attraverso la quale si tenta di carpire informazioni personali, dati finanziari o codici di accesso

3.4. Sito web della scuola.

La scuola ha un sito web, dove è possibile trovare tutte le informazioni e comunicazioni. Tutti i contenuti del settore didattico sono pubblicati direttamente sotto la supervisione della Dirigenza dell'Istituto che ne valuta la sicurezza e l'adeguatezza sotto i diversi profili dell'accessibilità, della pertinenza dei contenuti, del rispetto della privacy, ecc.

3.5. Social network.

Attualmente nella didattica non si utilizzano social network, neanche da parte dell'istituzione scolastica, e il personale scolastico non è autorizzato a utilizzarli in nome e per conto della stessa. La pubblicazione di nomi e giudizi sulle persone o sulle istituzioni e la diffusione di foto o filmati senza il consenso e, comunque, all'insaputa delle persone coinvolte può avere una rilevanza penale, come ad esempio la diffamazione. Non è consentito prelevare o diffondere immagini, video o registrazioni (anche solo audio) non autorizzate che contengano riferimenti offensivi, o comunque illeciti, nei confronti dell'istituto, dei docenti e degli studenti.

3.6. Protezione dei dati personali.

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), secondo quanto previsto dalle norme in vigore in materia di privacy e di tutela dei dati.

4. Strumentazione personale

4.1. Per gli studenti: gestione degli strumenti personali – cellulari, tablet, ecc.

Come da Regolamento di Istituto, è fatto divieto di utilizzare i telefoni cellulari in ambito scolastico, se non per scopi didattici (BYOD). Qualora i genitori ritengano indispensabile dotare il proprio figlio di un cellulare per mantenersi in contatto con lui al di fuori dell'orario delle lezioni, il telefono cellulare nell'ambiente scolastico deve essere tenuto assolutamente spento e riposto nello zaino.

L'uso del cellulare per riprese o foto non autorizzate e la loro eventuale pubblicazione in rete, oltre che essere oggetto di provvedimenti disciplinari per violazione del Regolamento interno, può costituire reato per violazione della privacy (Decreto legislativo 10 agosto

2018, n. 101 che adegua il Codice della Privacy, D.Lgs. 196/2003 alle disposizioni del Regolamento (UE) 2016/679 – GDPR e art.10 del Codice Civile) ed essere soggetto a possibili denunce presso l'autorità giudiziaria.
La scuola garantisce la possibilità di comunicazione tra le famiglie e gli alunni per urgenti motivi, mediante l'uso della linea telefonica della scuola.

4.2. Per i docenti: gestione degli strumenti personali – cellulari, tablet, ecc.

Durante le ore di lezione è consentito ai docenti l'uso di dispositivi elettronici personali, come il tablet, unicamente a scopo didattico e a integrazione dei dispositivi scolastici disponibili (il computer di classe), in special modo per l'utilizzo del registro elettronico.
Resta, comunque, il divieto di utilizzare i telefoni cellulari per comunicazioni personali, durante lo svolgimento delle attività di insegnamento.
Sono esonerati dal divieto dell'uso del cellulare soltanto i docenti collaboratori del Dirigente Scolastico e i docenti responsabili di plesso che, per motivi logistici ed organizzativi aventi carattere di eccezionalità e urgenza, dovranno essere comunque raggiungibili in qualsiasi momento.

4.3. Per il personale della scuola: gestione degli strumenti personali – cellulari, tablet, ecc.

Durante l'orario di servizio al restante personale scolastico l'uso del cellulare è consentito per comunicazioni personali urgenti.
L'uso di altri dispositivi elettronici personali è permesso solo per attività funzionali al servizio, e preventivamente autorizzato.

5. Prevenzione, rilevazione e gestione dei casi

5.1. Prevenzione

Al personale che opera nella scuola, e in modo particolare agli insegnanti, viene oggi offerta la possibilità di essere promotori e garanti della costruzione dialogica di un percorso formativo partecipato, ma il loro ruolo diventa spesso inevitabilmente quello di confidenti degli alunni e delle loro esperienze. Proprio per questo, gli insegnanti sono anche investiti del ruolo di sorta di "torre di avvistamento", avamposto privilegiato delle problematiche e dei rischi che bambini e adolescenti possono trovarsi ad affrontare ogni giorno. Basti pensare all'elevato numero di casi di bullismo e di cyberbullismo che gli insegnanti si trovano ad affrontare durante il loro insegnamento quotidiano.
La prima responsabilità degli insegnanti consiste, dunque, nell'imparare a **riconoscere** i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente.

Dall' a. s. 2021-22 l'Istituto ha inoltre avviato il progetto "Sportello psicopedagogico", a cura di esperti in problemi dell'età evolutiva. Il servizio, rivolto a famiglie, alunni e personale della scuola è finalizzato, tra le altre cose, ad intercettare malesseri connessi a casi di bullismo e cyberbullismo.

5.1.1. Rischi

I rischi che i ragazzi possono correre a scuola nell'utilizzo di dispositivi digitali possono derivare principalmente da un uso non corretto del telefono cellulare o di altri dispositivi come lo smartphone o il tablet. Sebbene, infatti, l'uso del cellulare e dello smartphone non sia consentito dal Regolamento dell'Istituto se non per momenti didattici, molti bambini della scuola primaria e quasi tutti i ragazzi della secondaria portano questi dispositivi che dovrebbero tenere spenti durante le lezioni. Accade purtroppo, che in orario scolastico, alcuni studenti, eludendo la sorveglianza del personale della scuola, accendano e adoperino il cellulare o lo smartphone, non solo per comunicare con i propri genitori, ma anche per navigare su internet, andando su siti non adatti e inviando materiali riservati (foto, video e altro). Così facendo, gli studenti possono incorrere anche a scuola nei rischi che abbiamo menzionato sopra, entrando in contatto e persino in confidenza con sconosciuti, fino a ricevere messaggi molesti e adescamenti.

Un'attenzione specifica andrà prestata ai seguenti fenomeni:

- **bullismo/cyberbullismo** – una forma di prepotenza virtuale attuata attraverso l'uso di internet e delle tecnologie digitali –;
- **sexting** - pratica di inviare o postare messaggi di testo e immagini a sfondo sessuale, come foto di nudo o semi-nudo, via cellulare o tramite Internet.
- **adescamento** o **grooming** – una tecnica di manipolazione psicologica, che gli adulti potenziali abusanti utilizzano online, per indurre i bambini/e o adolescenti a superare le resistenze emotive e instaurare una relazione intima e/o sessualizzata (Glossario di "Generazioni connesse").

5.1.2. Azioni

Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali possiamo individuare:

a) azioni da parte della scuola

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web, condividendo diversi materiali, tra cui quelli messi a disposizione sul sito del progetto "Generazioni connesse";
- richiedere di volta in volta autorizzazione esplicita da parte dei genitori all'utilizzo dei dati personali degli alunni (es. liberatoria per la pubblicazione di foto, immagini, video relativi al proprio/a figlio/a per la partecipazione a progetti didattici e altro);
- controllare periodicamente i siti visitati dagli alunni sui dispositivi scolastici;

b) azioni da parte dei docenti:

- seguire gli alunni nella navigazione in rete;
- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli studenti in orario scolastico se non per la metodologia BYOD;
- approfondire con attività mirate in classe, la conoscenza dei rischi derivanti dall'uso scorretto dei dispositivi tecnologici;

c) azioni da parte dei genitori:

- Firmare il patto di corresponsabilità redatto dalla scuola;
- Prendere visione della E-policy messa a disposizione sul sito della scuola www.icsalessandrinicesanob.edu.it
- Seguire le azioni promosse dalla scuola per un uso corretto della rete;

d) azioni da parte degli alunni:

- Prendere visione del patto di corresponsabilità che i genitori hanno firmato;
- Prendere visione della E-policy messa a disposizione sul sito della scuola www.icsalessandrinicesanob.edu.it
- Rispettare le regole per un uso corretto della tecnologia
- Denunciare qualsiasi caso di abuso;
- Partecipare agli eventi organizzati dalla scuola in materia di sicurezza on-line.

Azioni utili a impedire un utilizzo incauto, scorretto o criminoso degli strumenti digitali materiali inviati, scaricati, ricevuti o condivisi – su dispositivi digitali in uso a scuola (principalmente pc) sono:

5.2. Rilevazione

5.2.1. Che cosa segnalare

Tra i contenuti andranno opportunamente segnalati:

- dati sensibili o riservati (foto, immagini, video personali, informazioni private proprie di amici; l'indirizzo di casa o il telefono, ecc.);
- contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);
- contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale, come foto di nudo o semi-nudo, ecc.

5.2.2. Come segnalare: quali strumenti e a chi.

Mentre l'insegnante ha la possibilità, anzi il dovere, di intervenire sui dispositivi digitali in uso a scuola, non può intervenire direttamente sui telefoni cellulari dei bambini/alunni senza un'esplicita autorizzazione delle famiglie.

Il personale della scuola, anche con l'ausilio del personale di assistenza tecnica, dovrà:

a) provvedere a **conservare le eventuali tracce di una navigazione non consentita** su internet o del passaggio di materiali inidonei sui pc della scuola; la data e l'ora consentiranno di condurre più approfondite indagini; nel caso di messaggi, si cercherà di risalire al mittente attraverso i dati del suo profilo.

b) Darà **una tempestiva informazione delle famiglie in merito all'accaduto**, anche per consentire ulteriori indagini e, in assenza di prove oggettive, di raccogliere testimonianze sui fatti da riferire al Dirigente Scolastico ed, eventualmente, alla Polizia Postale.

Qualora siano coinvolti più alunni, in qualità di vittime o di responsabili della condotta scorretta, le famiglie degli alunni in questione saranno informate tempestivamente per un confronto.

Accertata l'entità dei fatti si provvederà:

1. a una comunicazione scritta tramite diario alle famiglie;
2. a una nota disciplinare sul Registro di classe;

3. a una convocazione formale dei genitori degli alunni, tramite segreteria;
4. a una convocazione delle famiglie da parte del Dirigente scolastico.

Per i reati più gravi la scuola si rivolgerà direttamente agli organi di polizia competenti.

5.3. Gestione dei casi

5.3.1. Definizione delle azioni da intraprendere a seconda della specifica del caso.

a) Casi di cyberbullismo:

Si definiscono bullismo tutte quelle situazioni caratterizzate da ***volontarie e ripetute aggressioni*** mirate a insultare, minacciare, diffamare e/o ferire una persona (o a volte un piccolo gruppo). Si tratta, pertanto, di una serie di comportamenti portati avanti ripetutamente nel tempo. Si parla di ***cyberbullismo*** quando queste forme di prevaricazione reiterate nel tempo si estendono anche alla vita online.

Tale specifica forma di bullismo ha caratteristiche peculiari:

1) è pervasivo: il bullo può raggiungere la sua vittima in qualsiasi momento e in qualunque luogo;
2) è un fenomeno persistente: il materiale messo online vi può rimanere per molto tempo;
3) spettatori e cyberbulli sono potenzialmente infiniti: le persone che possono assistere agli atti di cyberbullismo sono potenzialmente illimitate.

Occorre tenere presente che il cyberbullo non è mai del tutto consapevole della gravità dei suoi comportamenti se non viene aiutato ad esserne consapevole.

Qualora ci si trovi di fronte ad un caso di cyberbullismo si dovrà:

- informare i genitori degli alunni coinvolti;
- coinvolgere il referente di istituto dell'*e-policy* e gli operatori scolastici su quanto sta accadendo;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online.

b) Casi di sexting:

Qualora ci si trovi di fronte a un caso di sexting (con cui si intende l'invio e/o la ricezione e/o la condivisione di testi, video o immagini sessualmente esplicite via cellulare o tramite internet) si dovrà:

- Informare tempestivamente il Dirigente Scolastico;
- coinvolgere la classe e confrontarsi con esperti, facendo appello, per esempio, allo sportello d'ascolto dell'istituto per capire come approfondire e affrontare il fenomeno;
- coinvolgere la comunità scolastica in percorsi di prevenzione dei comportamenti riconducibili al *sexting*;

c) Casi di adescamento online o *grooming*:

Le tecnologie digitali consentono ai giovani di ampliare la propria rete di amicizie in modo quasi smisurato: non di rado gli adolescenti "concedono" la loro amicizia non solo a persone che conoscono direttamente, ma anche ad "amici di amici". Questo li espone arischi notevoli, come quello di dare accesso a sconosciuti al loro mondo online e quindi a informazioni personali.

L'adescamento online (*grooming*) consiste nel tentativo, da parte di un adulto, di avvicinare un/a bambino/a o adolescente per scopi sessuali, conquistandone la fiducia attraverso l'utilizzo della rete Internet (tramite chat, blog, forum e social networks,). In un primo tempo, l'adulto, spesso mentendo sulla propria identità e sulla propria età, mostra particolare interesse nei confronti del/la bambino/a o dell'adolescente, cercando di conquistarne la fiducia. Solo in un secondo tempo, cerca di entrare sempre più nell'intimità del bambino fino a introdurre argomenti intimi e attinenti alla sfera sessuale.

È bene che anche gli insegnanti aiutino i propri alunni a tutelarsi, scegliendo con cura chi frequentare online, per evitare che una condotta imprudente possa comportare ripercussioni non banali nella loro vita reale.

Una volta riconosciuti alcuni segni che possono rinviare a una situazione di adescamento online, quali un improvviso calo nel rendimento scolastico; un aumento del tempo trascorso dall'alunno online congiunto ad una particolare riservatezza al riguardo; allusioni da parte dell'alunno alla frequentazione di una persona più grande, o a regali ricevuti, ecc., è bene:

- informare tempestivamente il Dirigente Scolastico;
- approfondire la situazione coinvolgendo la classe e l'intera comunità scolastica;
- avviare dei percorsi di riflessione in classe sul concetto di fiducia;
- farsi affiancare da esperti, ricorrendo anche allo sportello d'ascolto per offrire ai minori, qualora lo desiderino, il supporto necessario.

Allegati

Allegato 1_Protocollo di azione contro bullismo e cyberbullismo relativi sub allegati:

1.1 Scheda di prima segnalazione prepotenze, bullismo, cyber-bullismo: scheda utilizzabile da tutto il personale scolastico, dai genitori, dagli alunni, per segnalare episodi di prepotenza ritenuti di grado medio/grave. Utile a ricostruire e analizzare il fatto compiuto.

1.2 Scheda di valutazione approfondita: utile al Referente bullismo e cyber bullismo e al Consiglio di Classe per definire e descrivere in modo dettagliato l'episodio di bullismo/cyber-bullismo, di registrare gli interventi decisi e gli esiti del monitoraggio successivo.

1.3 QUESTIONARIO SELF-REPORT_Florence Bullying Victimization Scales - QUESTIONARIO SELF-REPORT_Florence Cyberbullying Cybervictimization Scales - QUESTIONARIO SELF REPORT_ La mia vita a scuola-: Utili come fonte di informazione fondamentale rispetto alla frequenza, alla tipologia e alla modalità di manifestazione dei casi di BULLISMO, VITTIMIZZAZIONE e più i generale dei RUOLI che i ragazzi possono assumere in una situazione di bullismo.

1.4 Scheda per il monitoraggio: utile per l'osservazione e la valutazione (a breve termine o a lungo termine) del comportamento di tutti gli alunni coinvolti con possibilità di interventi educativi di rinforzo.

1.5 Modello per la segnalazione in materia di cyber-bullismo al garante per la protezione dei dati personali: utile agli ultraquattordicenni e ai

genitori degli alunni al di sotto dei 14 anni, per richiedere il blocco o l'oscuramento dei dati che possono ledere i poss4essori minorenni.

1.6 Modello di istanza di ammonimento: scheda utile a chiedere al Questore l'ammonimento all'autore della condotta molesta reiterata nel tempo.

Procedure operative per la rilevazione, il monitoraggio e la gestione delle segnalazioni

Le procedure, da applicarsi secondo i criteri e le modalità specifiche dettati dalla policy, sono incluse nel Regolamento di Istituto e nei suoi allegati.

Cesano Boscone, il 22/04/2022

L'Animatore Digitale
Prof. Simone Manfredda

Il Dirigente Scolastico
Dott.ssa Mariangela Camporeale