Ultimo aggiornamento - CDU del 02/03/2022

Documento di ePolicy

ATIC80600E

VILLANOVA D'ASTI

VIA ZABERT 14 - 14019 - VILLANOVA D'ASTI - ASTI (AT)

CLAUDIA SARDELLI

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

L'E-policy ha l'obiettivo di esprimere la nostra visione educativa e proposta formativa, in riferimento alle tecnologie digitali. Nello specifico:

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

Argomenti del Documento

Perché è importante dotarsi di una E-policy?

Attraverso l'E-policy il nostro Istituto si vuole dotare di uno strumento operativo a cui tutta la comunità educante dovrà fare riferimento, al fine di assicurare un approccio alla tecnologia che sia consapevole, critico ed efficace, e al fine di sviluppare, attraverso specifiche azioni, una conoscenza delle opportunità e dei rischi connessi all'uso di Internet.

L' E-policy fornisce, quindi, delle linee guida per garantire il benessere in Rete, definendo regole di utilizzo delle TIC a scuola e ponendo le basi per azioni formative e educative su e con le tecnologie digitali, oltre che di sensibilizzazione su un uso consapevole delle stesse.

L'E-SAFETY ingloba tecnologia internet e comunicazione elettronica come telefoni cellulari e tecnologia wireless, sottolinea la necessità di educare i bambini e gli adolescenti sui benefici e i rischi dell'uso delle tecnologie e fornisce salvaguardia e consapevolezza a chi le usa, permettendo loro di controllare da soli le proprie esperienze online.

L' E-SAFETY POLICY (* da adesso abbreviato ESP) della scuola opererà in comunione con le altre politiche relative al comportamento degli studenti, bullismo, cyberbullismo, curricolo, protezione dei dati e sicurezza.

Lo scopo di questa politica è di:

• stabilire i principi fondamentali di tutti i membri della comunità scolastica dell'Istituto Comprensivo di Villanova d'Asti per quanto riguarda l'utilizzo di tecnologie basate sulle TIC

• salvaguardare e proteggere gli studenti e il personale scolastico

• assistere il personale della scuola che interagisce con gli studenti, nel lavorare in modo sicuro e responsabile con le TIC monitorando i propri standard e le prassi

• impostare chiare aspettative di comportamento e / o codici di condotta rilevanti per un uso responsabile di Internet ai fini didattici, personali o ricreativi

• definire procedure chiare per affrontare gli abusi online come cyberbullismo, in riferimento incrociato con le altre politiche della scuola

• prevenire comportamenti illeciti o pericolosi e intraprendere opportuni provvedimenti in caso di infrazione.

1.2 - Ruoli e responsabilità

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

La scuola ha un team digitale che lavora al continuo aggiornamento del documento E-safety Policy.

La nostra E-SAFETY POLICY è stata redatta dal gruppo di lavoro e approvata dal Dirigente Scolastico e dal Collegio dei Docenti. Questa E-SAFETY POLICY verrà rinnovata ogni anno. Il prossimo aggiornamento è previsto per novembre 2022.

RUOLO RESPONSABILITA'

RUOLO	RESPONSABILITA'
Dirigente scolastico	• responsabilità globale della e-safety • responsabilità dei dati sensibili e dati relativi alla sicurezza • assicura che la scuola utilizzi un Internet Service approvato che sia conforme ai requisiti di legge • assicura che il personale addetto alla sicurezza su Internet riceva formazione permanente
	• é a conoscenza delle procedure da seguire in caso di eventuali incidenti relativi alla sicurezza su internet o e safety (*da adesso abbreviato ES). • riceve relazioni periodiche di monitoraggio dai responsabili del ESP
Referenti e-safety	• assumono la responsabilità quotidiana sulle questioni di ES e hanno un ruolo di primo piano nella definizione e revisione delle politiche e dei documenti di ES • promuovono la consapevolezza e l'impegno per la salvaguardia

	relativa alle tecnologie di tutta la comunità scolastica

	• assicurano che l'istruzione e la sicurezza vengano incorporate nel curricolo scolastico • coordinano e mantengono contatti con i docenti, con le autorità e gli enti esperti per discutere le questioni, redigere e aggiornare i registri degli incidenti, relazionare periodicamente il lavoro del gruppo con la dirigenza • operano affinché tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidenti • si tengono aggiornati riguardo alla legislazione in materia di ES ed è consapevole dei potenziali problemi derivanti da: - condivisione di dati personali - accesso ai materiali illegali / inadeguati - inadeguato contatto on-line con adulti / sconosciuti - incidenti potenziali o reali di adescamento - cyberbullismo e uso dei social media

Animatore digitale	• stimola la formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di laboratori formativi (senza essere necessariamente un formatore), favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative, come ad esempio quelle organizzate attraverso gli snodi formativi • favorisce la partecipazione e stimola 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 • individua 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; la pratica di una metodologia comune; informazione su innovazioni esistenti in altre scuole; un 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. • Forma in materia di utilizzo appropriato delle TIC

Polizia Postale - Carabinieri Psicologa della scuola	• Incontri di formazione /informazione per genitori, alunni e insegnanti • Interventi in caso di incidenti • Consulenza • Counseling • Sportello di ascolto per gli studenti e genitori • Incontri di prevenzione dei rischi • Incontri formativi / informativi per insegnanti e genitori

Tecnico	• Fornisce e supporta il funzionamento delle apparecchiature TIC e del sistema di filtraggio • Forma in materia di utilizzo appropriato delle TIC
Insegnanti	• incorporano i temi di ES nel programma di studi e nelle attività scolastiche • supervisionano e guidano gli alunni nelle attività di apprendimento che coinvolgono tecnologia on-line • operano affinchè gli alunni siano consapevoli degli aspetti giuridici riguardanti i contenuti elettronici, quali le leggi sul copyright, ecc. • sono consapevoli dei problemi di sicurezza correlati all'uso di telefoni cellulari, fotocamere e dispositivi portatili, ne monitorano l'utilizzo e mettono in atto le politiche scolastiche vigenti in materia • segnalano qualsiasi abuso sospetto o problema al Team Digitale
Tutto il personale	• legge e contribuisce a promuovere politiche di ES della scuola • legge, firma e aderisce alla ESP • è consapevole dei problemi di sicurezza correlati all'uso di telefoni cellulari, fotocamere e dispositivi portatili, ne monitora l'utilizzo e mette in atto le politiche scolastiche vigenti in materia

	• segnala qualsiasi abuso sospetto o problema al coordinatore di e-safety • favorisce comportamenti sicuri, responsabili e professionali nell'utilizzo della tecnologia • fa in modo che le comunicazioni digitali con gli allievi avvengano in modo professionale e solo attraverso sistemi adottati e approvati dalla scuola

Studenti	• Leggono, firmano e aderiscono alla ESP della scuola e al patto di corresponsabilità ES • utilizzano le TIC ai fini delle attività scolastiche evitando il plagio e rispettando le normative sul diritto d'autore • comprendono l'importanza di segnalare abusi, usi impropri o accessi a materiali inappropriati • sanno quali azioni intraprendere nel caso in cui loro stessi o qualcuno di loro conoscenza si trovi in situazione di rischio o disagio • conoscono e comprendono la politica della scuola sull'uso dei telefoni cellulari, fotocamere digitali e dispositivi portatili • conoscono e comprendono la politica scolastica relativa all'uso di immagini e al cyberbullismo • conoscono i vantaggi e i rischi dell'utilizzo di Internet e delle altre tecnologie • collaborano nella creazione / revisione delle politiche di ES

Genitori	• leggono, firmano e aderiscono alla ESP della scuola e al patto di corresponsabilità ES • sostengono la scuola nel promuovere ESP • leggono e promuovono l'accordo che l'allievo sottoscrive con la scuola riguardo alla ESP • collaborano con la scuola nel caso ci siano preoccupazioni riguardo all'uso della tecnologia da parte dei propri figli
Gruppi esterni	• Ogni individuo / organizzazione esterna, prima di usare qualsiasi apparecchiatura o Internet all'interno della scuola deve essere al corrente della ESP e condividerne il contenuto

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

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

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

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

1.4 - Condivisione e comunicazione dell’ePolicy all’intera comunità scolastica

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

documento.

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

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

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

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

ALUNNI

• Gli alunni saranno informati della policy dagli insegnanti, dal sito web della scuola e attraverso diario scolastico

• Gli studenti saranno avvisati che l’uso di internet potrà essere monitorato PERSONALE

• A tutto il personale sarà fornita la policy attraverso l’area riservata del sito di Istituto e tramite mail

• Il personale deve essere consapevole che il traffico di Internet potrebbe essere monitorato con la possibilità di risalire alla connessione del singolo dispositivo

GENITORI
• Un estratto del documento ESP e del patto di corresponsabilità ES sarà portato all’attenzione dei genitori tramite il diario scolastico con la possibilità di consultare il documento in versione integrale sul sito della scuola

1.5 - Gestione delle infrazioni alla ePolicy

La scuola gestirà le infrazioni all’E-policy attraverso azioni educative e/o sanzioni, qualora fossero necessarie, valutando i diversi gradi di gravità di

eventuali violazioni.

VALUTAZIONE DEI RISCHI

La scuola prenderà tutte le precauzioni necessarie per impedire l'accesso inappropriato a materiale o per tutelare la riservatezza dei dati personali, tuttavia data la vastità della rete non è possibile garantire che ciò avvenga sempre.

La scuola farà in modo che la politica di ES sia adeguata e la sua attuazione appropriata.

GESTIONE DEI RECLAMI SULLA SICUREZZA INFORMATICA

Qualsiasi lamentela personale ed abuso deve essere riferita al Dirigente Scolastico o persona da questi delegata

Gli alunni e i genitori saranno informati della procedura di segnalazione e gestione degli incidenti informatici

I problemi più gravi saranno affrontati con gli organi competenti: polizia postale, carabinieri, ecc.

1.6 - Integrazione dell'ePolicy con Regolamenti esistenti

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

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO

CHECKLIST

	SI - NO	NOTE
La protezione dei dati personali è sicura	SI	
Il sito della scuola è fornito di crittografia	NO	
La sicurezza delle password è efficace	IN PARTE	DA MIGLIORARE
La policy della scuola è dettagliata e aggiornata	SI	

I principi fondanti dell'ESP sono presenti all'interno del curricolo scolastico	SI	
C'è un sistema di filtraggio o di monitoraggio sulla rete per la connessione ad internet	SI	
C'è evidenza di formazione dello staff	SI	
Gli studenti sono a conoscenza di come e a chi riportare un problema	NO	

Indicatori di buone pratiche:

		INDICARE UN VALORE DA 1 A 4 (dove 1=poco e 4=molto)
Approccio coerente di tutta la scuola	Tutti docenti e non docenti sono in grado di riconoscere e sono consapevoli dei problemi riguardo la sicurezza.	2
	La formazione in materia di ES è estesa e le competenze del personale sono vaste.	1
	Il contributo degli alunni, dei genitori e della comunità scolastica è presente e integrato.	1
Solida ed integrata routine di report	I percorsi scolastici da utilizzare per le segnalazioni sono compresi chiaramente e utilizzati da tutta la scuola.	2
	Esiste un uso efficace di peer mentoring e sostegno.	3

Staff	Tutto il personale docente e non docente riceve regolare formazione ed aggiornamento.	3
	Uno o più membri del personale hanno un alto livello di competenza e responsabilità chiaramente definite.	3
Policies	Rigorose politiche e procedure di ES sono in atto, scritte in italiano semplice e aggiornate regolarmente.	3

	La politica ESP è integrata con gli altri regolamenti di Istituto.	4
	La politica di ES è compresa e rispettata da allievi, personale e genitori.	3

Istruzione	Esiste un curricolo relativo all'ES adatto all' età degli allievi che viene utilizzato per promuovere le buone pratiche di uso responsabile delle rete e delle TIC nel rispetto della propria e altrui sicurezza.	4
Infrastruttur e	La scuola utilizza un Internet Service Provider o piano a banda larga.	4
	La scuola possiede un sistema di filtraggio correlato all'età che viene monitorato attivamente.	4
Monitorag gio e valutazion e	La valutazione del rischio viene utilizzata con buoni risultati nella promozione di ES.	3
	L'utilizzo dei dati di monitoraggio è efficace per valutare l'impatto delle pratiche di ES e per realizzare strategie di azione.	3
Gestione dei dati personali	L'importanza della salvaguardia dei dati personali è compresa e i dati sono gestiti in modo sicuro e in conformità con i requisiti di legge.	4

Questo veloce self-audit aiuterà a valutare se i principi di base della ESP sono a corretti e aggiornati.

	SI - NO	NOTE
La scuola ha una ESP conforme alle linee guida?	Sì	

Data dell'ultimo aggiornamento 30 ottobre 2021	SI	
La policy è stata approvata in data 26 ottobre 2021		
La policy è a disposizione dello staff nell'area riservata del sito web di istituto: https://icvillanovasti.edu.it	SI	

E per le famiglie nell'area genitori del sito web di istituto: https://icvillanovasti.edu.it		
E' stata fornita una formazione sulla ESP sia allo staff che agli studenti?	SI	
E' stato condiviso da parte del personale un codice di condotta sulle TIC?	IN PARTE	
E' stato firmato dalle famiglie e restituito alla scuola un patto di corresponsabilità ESP?	SI	
Sono state fissate delle regole sulla ESP per gli studenti?	SI	
Sono state appese in modo visibile in tutte le stanze con computer e nelle aule?	SI	
L'accesso ad internet è fornito da un provider approvato che rispetta le linee guida della sicurezza?	SI	
La scuola ha una politica di filtraggio approvata?	SI	
I dati personali e documenti sono immagazzinati e usati in accordo con i principi della legge sulla privacy?	SI	

Il nostro piano d'azioni

FORMAZIONE DEI DOCENTI SULL'UTILIZZO E L'INTEGRAZIONE DELLE TIC NELLA DIDATTICA.

Il concreto utilizzo delle TIC in classe come elemento innovativo non dipende solamente dall'effettiva e funzionale dotazione strumentale, ma anche e soprattutto dalla capacità di comprenderne le potenzialità rispetto a contesti e finalità specifici. Per sostenere un processo di consapevole innovazione didattica è necessario investire sulla formazione e l'aggiornamento degli insegnanti.

La nostra scuola supporta la formazione dei docenti in servizio attraverso:

• L'organizzazione di corsi interni

• La partecipazione a reti di scuole che effettuano anche percorsi di formazione

• La diffusione tramite sito web di informazioni su corsi sia gratuiti che a pagamento organizzati da diversi enti

FORMAZIONE DEI DOCENTI SULL'UTILIZZO CONSAPEVOLE E SICURO DI INTERNET E DELLE TECNOLOGIE DIGITALI

Questa scuola:

• supporta la formazione del personale in materia di ES con aggiornamenti annuali, riunioni del personale ecc.

• forma il personale affinchè sappia custodire i dati sensibili, inviarli o riceverli in modo sicuro, secondo norma di legge;

• fornisce a tutto il nuovo personale informazioni e indicazioni sulla ESP della scuola

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali". Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).

Per questo la scuola si impegna a portare avanti percorsi volti a promuovere tali competenze, al fine di educare gli studenti e le studentesse verso un uso consapevole e responsabile delle tecnologie digitali. Ciò avverrà attraverso la progettazione e implementazione di un curricolo digitale.

2.2 - Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica

È fondamentale che i docenti tutti siano formati ed aggiornati sull'uso corretto, efficace ed efficiente delle TIC nella didattica, al fine di usarle in modo integrativo ed inclusivo.

Ciò si rende necessario per fornire agli studenti e alle studentesse modelli di utilizzo positivo, critico e specifico delle nuove tecnologie e per armonizzare gli apprendimenti.

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

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

2.4. - Sensibilizzazione delle famiglie e integrazioni al Patto di Corresponsabilità

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

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020)

Scegliere almeno 1 di queste azioni

Effettuare un'analisi del fabbisogno formativo su un campione

di studenti e studentesse in relazione alle competenze digitali.

Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo e l’integrazione delle TIC nella didattica.

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

AZIONI (da sviluppare nell’arco dei tre anni scolastici successivi)

Scegliere almeno 1 di queste azioni

Effettuare un’analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.

Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo e l’integrazione delle TIC nella didattica.

Effettuare un’analisi del fabbisogno formativo del corpo docente sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell’ambito dell’educazione alla cittadinanza digitale.

Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo e l’integrazione delle TIC nella didattica. Organizzare e promuovere per il corpo docente incontri formativi sull’utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

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

3.1 - Protezione dei dati personali

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

(cfr. http://www.garanteprivacy.it/scuola).

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

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

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

In questo paragrafo dell'ePolicy affrontiamo tale problematica, con particolare

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

3.2 - Accesso ad Internet

1. *L'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.*
2. *Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale.*
3. *Il diritto fondamentale di accesso a Internet deve essere assicurato nei suoi presupposti sostanziali e non solo come possibilità di collegamento alla Rete.* 4. *L'accesso comprende la libertà di scelta per quanto riguarda dispositivi, sistemi operativi e applicazioni anche distribuite.*
5. *Le Istituzioni pubbliche garantiscono i necessari interventi per il superamento di ogni forma di divario digitale tra cui quelli determinati dal genere, dalle condizioni economiche oltre che da situazioni di vulnerabilità personale e disabilità.*

Così recita l'art. 2 della Dichiarazione dei diritti di Internet, elaborata dalla Commissione per i diritti e i doveri in Internet, commissione costituita il 27 ottobre 2014 presso la Camera dei Deputati dalla presidente Laura Boldrini e presieduta da Stefano Rodotà. Inoltre, il 30 aprile 2016 era entrato in vigore il Regolamento UE del Parlamento Europeo e del Consiglio del 25 novembre 2015, che stabilisce le "misure riguardanti l'accesso a un'Internet aperto e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

Il diritto di accesso a Internet è dunque presente nell'ordinamento italiano ed europeo e la scuola dovrebbe essere il luogo dove tale diritto è garantito, anche per quegli studenti che non dispongono della Rete a casa. In modo coerente il PNSD (Piano Nazionale Scuola Digitale) ha tra gli obiettivi quello di "fornire a tutte le scuole le condizioni per l'accesso alla società dell'informazione e fare in modo che il "diritto a Internet" diventi una realtà, a partire dalla scuola".

Questo perché le tecnologie da un lato contribuiscono a creare un ambiente che può rendere la scuola aperta, flessibile e inclusiva, dall'altro le consentono di adeguarsi ai cambiamenti della società e del mercato del lavoro, puntando a sviluppare una cultura digitale diffusa che deve iniziare proprio a scuola.

3.3 - Strumenti di comunicazione online

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

3.4 - Strumentazione personale

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

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

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

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

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

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

Organizzare uno o più eventi o attività volti a formare i genitori dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali

Organizzare uno o più eventi o attività volti a formare il personale adulto dell'Istituto sui temi dell'accesso ad Internet e dell'uso sicuro delle tecnologie digitali (cybersecurity)

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

Capitolo 4 - Rischi on line: conoscere, prevenire e rilevare

4.1 - Sensibilizzazione e Prevenzione Il

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

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

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

Gli strumenti da adottare per poter ridurre l'incidenza di situazioni di rischio si configurano come interventi di **sensibilizzazione e prevenzione.**

Nel caso della **sensibilizzazione** *si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.*

Nel caso della **prevenzione** *si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.*

4.2 - Cyberbullismo: che cos'è e come prevenirlo

La legge 71/2017 "Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo", nell'art. 1, comma 2, definisce il cyberbullismo:

"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".

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

formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;

sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015); promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;

previsione di misure di sostegno e rieducazione dei minori coinvolti; Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;

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

Nomina del Referente per le iniziative di prevenzione e contrasto che: Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.

Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

4.3 - Hate speech: che cos'è e come prevenirlo

Il fenomeno di "incitamento all'odio" o "discorso d'odio", indica discorsi (post, immagini, commenti etc.) e pratiche (non solo online) che esprimono odio e intolleranza verso un gruppo o una persona (identificate come appartenente a un gruppo o categoria) e che rischiano di provocare reazioni violente, a catena. Più ampiamente il termine "hate speech" indica un'offesa fondata su una qualsiasi discriminazione (razziale, etnica, religiosa, di genere o di orientamento sessuale, di disabilità, eccetera) ai danni di una persona o di un gruppo.

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;

promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;

favorire una presa di parola consapevole e costruttiva da parte dei giovani.

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere in relazione a questa problematica.

4.4 - Dipendenza da Internet e gioco online

La Dipendenza da Internet fa riferimento all'utilizzo eccessivo e incontrollato di Internet che, al pari di altri comportamenti patologici/dipendenze, può causare o essere associato a isolamento sociale, sintomi da astinenza, problematiche a livello scolastico e irrefrenabile voglia di utilizzo della Rete.

L'istituto è intenzionato a promuovere azioni di prevenzione attraverso percorsi sul benessere digitale?

4.5 - Sexting

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

4.6 - Adescamento online

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

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

In Italia l’adescamento si configura come reato dal 2012 (art. 609-undecies – l’adescamento di minorenni) quando è stata ratificata la Convenzione di Lanzarote (legge 172 del 1° ottobre 2012).

A seguire vengono descritte le azioni che il nostro Istituto intende intraprendere per prevenire ed affrontare la delicata problematica dell’adescamento.

4.7 - Pedopornografia

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

o simulate o qualsiasi rappresentazione degli organi sessuali a fini soprattutto sessuali.

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

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

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

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

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

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

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2019/2020).

□ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse,

con il coinvolgimento di esperti.

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

□ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

□ Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

□ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

□ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

□ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

AZIONI (da sviluppare nell'arco dei tre anni scolastici successivi).

□ Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi

associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.

□ Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

□ Organizzare uno o più incontri di formazione all'utilizzo sicuro e consapevole di Internet e delle tecnologie digitali integrando lo svolgimento della didattica e assicurando la partecipazione attiva degli studenti/studentesse.

□ Promuovere incontri e laboratori per studenti e studentesse dedicati all' Educazione Civica Digitale.

□ Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di

cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

□ Organizzare laboratori di educazione alla sessualità e all'affettività, rivolti agli/lle studenti/studentesse.

□ Organizzare uno o più eventi e/o dibattiti in momenti extra-scolastici, sui temi della diversità e sull'inclusione rivolti a genitori, studenti/studentesse e personale della scuola.

□ Pianificare e realizzare progetti di peer-education - sui temi della sicurezza online - nella scuola.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

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

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

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e**

servizi presenti sul territorio (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

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

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

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

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

Cyberbullismo: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).

Adescamento online: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.

Sexting: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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

Vi suggeriamo, inoltre, i seguenti servizi:

- Servizio di Helpline 19696 e Chat di Telefono Azzurro per supporto ed emergenze;

- Clicca e segnala di Telefono Azzurro e STOP-IT di Save the Children Italia per

segnalare la presenza di materiale pedopornografico online.

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

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

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

Strumenti a disposizione di studenti/esse

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

un indirizzo e-mail specifico per le segnalazioni;

scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;

sportello di ascolto con professionisti;

docente referente per le segnalazioni.

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto

Riferimenti normativi e sanzioni disciplinari

Al fine di prevenire episodi spiacevoli dovuti a un uso improprio e illecito dello smartphone, riteniamo opportuno sottolineare che il nostro Istituto vieta agli allievi l'uso del telefono cellulare (o di altro dispositivo ad esso assimilabile per le funzioni di cui è dotato) nelle sue pertinenze, dentro e fuori dalle aule (bagni, corridoi, palestra, cortili, etc.), durante le lezioni o in qualunque altro momento della giornata scolastica.

Il docente, a sua discrezione, potrà consentirne l'uso per esigenze didattiche e/o particolari necessità contingenti di comunicazione dell'allievo con l'esterno. Si ricorda, comunque, che le linee telefoniche della scuola sono sempre disponibili per qualunque urgenza.

È utile soffermarsi sugli aspetti normativi che regolano l'uso del telefono a scuola e sulle possibili conseguenze legali inerenti a un uso non corretto delle funzioni di cui questi dispositivi sono dotati (sms, chat, social, foto, video, etc,).

Dall'**art. 3 del D.P.R. n. 249 del 24 giugno 1998** (Regolamento recante lo "Statuto delle studentesse e degli studenti della scuola secondaria") e s.m.i. (**D.P.R. n. 235 del 21 novembre 2007**), si evince la sussistenza di un dovere specifico, per ciascuno studente, di non utilizzare il telefono cellulare, o altri dispositivi elettronici, durante lo svolgimento delle attività didattiche.

La **nota del Ministero della Pubblica Istruzione del 15 marzo del 2007** avente ad oggetto "Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, irrogazione di sanzioni disciplinari, dovere di vigilanza e di corresponsabilità‡ dei genitori e dei docenti." recita testualmente:

"In via preliminare, è del tutto evidente che il divieto di utilizzo del cellulare durante le ore di lezione risponda ad una generale norma di correttezza che, peraltro, trova una sua codificazione formale nei doveri indicati nello Statuto delle studentesse e degli studenti, di cui al D.P.R. 24 giugno 1998, n. 249.

In tali circostanze, l'uso del cellulare e di altri dispositivi elettronici rappresenta un elemento di distrazione sia per chi lo usa che per i compagni, oltre che una grave mancanza di rispetto per il docente configurando, pertanto, un'infrazione disciplinare sanzionabile attraverso provvedimenti orientati non solo a prevenire e scoraggiare tali comportamenti ma anche, secondo una logica educativa propria dell'istituzione scolastica, a stimolare nello studente la consapevolezza del
disvalore dei medesimi."

Particolare attenzione, inoltre, deve essere posta a tutela della privacy, con particolare riferimento all'utilizzo dei telefoni cellulari o di altri dispositivi elettronici quando questi hanno lo scopo di acquisire e/o divulgare immagini, filmati o registrazioni vocali. A questo riguardo, viene in soccorso la **Direttiva n. 104 del 30 novembre 2007 del Ministero della Pubblica Istruzione** che al **punto 4** recita:

"[…] comportamenti, connessi ad un trattamento improprio di dati personali acquisiti mediante telefoni cellulari o altri dispositivi elettronici, devono essere sanzionati con opportuno rigore e severità nell'ambito dei regolamenti delle singole istituzioni scolastiche."

Si rammenta che chi abusa dell'immagine altrui contravviene all'**art. 10 del Codice Civile**, agli **artt. 96 e 97 della L. 633 del 22 aprile 1941 sul diritto d'autore**, nonché agli **artt. 13, 23, 161 e 166 del D. Lgs. 196/2003 (Codice della Privacy)**, successivamente adeguato al Regolamento (UE) 2016/679 dal D. Lgs. 101/2018.

Chi utilizza dati personali (immagini, filmati, registrazioni vocali, etc.), raccolti con il proprio cellulare o altri dispositivi, deve vagliare tutte le circostanze e porre attenzione a che i propri comportamenti non ledano i diritti dei terzi. Alcune leggerezze potrebbero, infatti, configurare anche delle fattispecie di reato punite, ad esempio, dagli **artt. 528, 594, 600-ter, 615-bis del Codice Penale**, la cui descrizione preferiamo qui omettere.

Si ricorda, inoltre, che ai sensi dell'**art. 2048 del Codice Civile** "*Il padre e la madre, o il tutore, sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati*" e che l'articolo stesso pone a loro carico **la presunzione di responsabilità**. In sinergia con l'**art. 30 della Costituzione** e con l'**art. 147 del Codice Civile**, in merito all'obbligo di educazione dei figli, numerose sentenze della Cassazione interpretano univocamente le intenzioni del legislatore. Tali sentenze sostengono, infatti, che per poter essere liberato dalla responsabilità dei fatti, il genitore dovrà non soltanto dimostrare "*[…] di aver adempiuto tutti i doveri ed*

esercitato tutti i poteri normalmente idonei ad impedire la illecita condotta del figlio […]" **(Cass. 22/11/78 n. 5465)**, ma anche "[…] dimostrare di avere impartito al minore una educazione ed un'istruzione consone alle proprie condizioni sociali e familiari e di avere altresì vigilato sulla sua condotta in maniera adeguata all'ambiente, alle attitudini e al carattere del soggetto." **(Cass. 28/10/78 n. 4937)**.

I genitori, inoltre, per andare esenti da responsabilità dovranno ancora provare di avere impartito ai loro figli anche una ***"educazione dei sentimenti e delle emozioni"***: non è sufficiente dimostrare di avere impartito messaggi educativi, ma è necessario verificare anche l'avvenuta assimilazione da parte dei figli dei valori trasmessi.

Si invitano, pertanto, i genitori a collaborare fortemente con la scuola, in un'alleanza educativa, alla sensibilizzazione dei ragazzi, all'uso corretto del telefono cellulare, affinché ne comprendano i rischi derivanti da un uso improprio, in un'ottica formativa del cittadino di domani.

Tenendo conto di tutto quanto su esposto e del **D.P.R. n. 235 del 21 novembre 2007** (*"Statuto delle studentesse e degli studenti della scuola secondaria"*) che modifica e integra il **D.P.R. n. 249 del 24 giugno 1998** e che all'**art. 4 comma 5** così recita:

"*Le sanzioni sono sempre temporanee, proporzionate alla infrazione disciplinare e ispirate al principio di gradualità nonché, per quanto possibile, al principio della riparazione del danno. Esse tengono conto della situazione personale dello studente, della gravità del comportamento e delle conseguenze che da esso derivano. Allo studente è sempre offerta la possibilità di convertirle in attività in favore della comunità scolastica.*",

si elencano qui di seguito i provvedimenti disciplinari previsti dal nostro regolamento in caso di uso non autorizzato del cellulare nei locali della scuola e nelle sue pertinenze.

Per non rischiare di infrangere il regolamento e di incappare così nelle sanzioni previste, l'allievo dovrà quindi accertarsi di avere il telefono spento, ricordandosi che **non è ammessa neppure la modalità aereo**.

Se l'allievo dimentica di spegnere il telefono e chiede spontaneamente di farlo prima che il docente se ne accorga, allora lo si esorterà verbalmente a una maggiore attenzione.

Se il telefono dell'allievo è acceso (evento segnalato, ad esempio, a causa di un segnale acustico emesso dallo stesso), **la prima volta** il docente inviterà allo spegnimento del dispositivo, valutando l'opportunità di segnalare l'accaduto ai genitori tramite diario.

Se il telefono dell'allievo è acceso (evento segnalato, ad esempio, a causa di un segnale acustico emesso dallo stesso), **la volta successiva** (avendo contezza della precedente) il docente inviterà allo spegnimento del dispositivo, segnalerà l'accaduto ai genitori tramite diario e valuterà, inoltre, l'opportunità di annotare l'episodio anche sul registro di classe.

Se l'allievo usa il proprio telefono per parlare, per navigare in internet, per chattare, per andare sui social, per registrare audio e/o video, per scattare foto, etc., il docente, a sua discrezione, scriverà una nota disciplinare sul registro di classe, comunicandolo alla famiglia tramite il diario. Dopo avere intimato lo spegnimento del dispositivo, il docente valuterà inoltre l'opportunità di ritirare il telefono per restituirlo o a fine ora, o a fine lezioni (in questo caso sarà depositato al sicuro in bidelleria, inserito in apposita busta), o solamente quando il genitore verrà a ritirarlo personalmente previa convocazione telefonica. In questo ultimo caso, si inviterà allora l'allievo a estrarre la SIM dal telefono, dopodiché lo si inserirà in un'apposita busta e lo si custodirà in segreteria fino all'arrivo del genitore.

Se l'allievo usa il proprio telefono per acquisire e/o divulgare immagini, filmati, registrazioni vocali, etc., ledendo diritti di terzi, il docente scriverà una nota disciplinare sul registro di classe, comunicandolo alla famiglia tramite diario. Il Consiglio di Classe, inoltre, con "*opportuno rigore e severità*" richiamati dal **punto 4** della **Direttiva n. 104 del 30 novembre 2007 del Ministero della Pubblica Istruzione**, potrà decidere se comminare all'allievo una sanzione disciplinare di sospensione dalle lezioni di uno o più giorni (fino a un massimo di tre) con l'obbligo di frequenza. La sanzione potrà, comunque, essere commutata nello svolgimento di attività "riparatorie" di rilevanza sociale o di interesse generale per la comunità stabilite dal Dirigente Scolastico e/o dal Consiglio di Classe.

Si ricorda, infine, che eventi che ledono i diritti di terzi, come il caso appena citato, **possono sempre essere denunciati alle autorità competenti**.

5.3. - Gli attori sul territorio

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

Per una mappatura degli indirizzi di tali strutture è possibile consultare il Vademecum di Generazioni Connesse "Guida operativa per conoscere e orientarsi nella gestione di alcune problematiche connesse all'utilizzo delle tecnologie digitali da parte dei più giovani" (seconda parte, pag. 31), senza dimenticare che la Helpline di Telefono Azzurro (19696) è sempre attiva nell'offrire una guida competente ed un supporto in tale percorso.

A seguire i principali Servizi e le Agenzie deputate alla presa in carico dei vari aspetti che una problematica connessa all'utilizzo di Internet può presentare.

Comitato Regionale Unicef: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.

Co.Re.Com. (Comitato Regionale per le Comunicazioni): svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.

Ufficio Scolastico Regionale: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.

Polizia Postale e delle Comunicazioni: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.

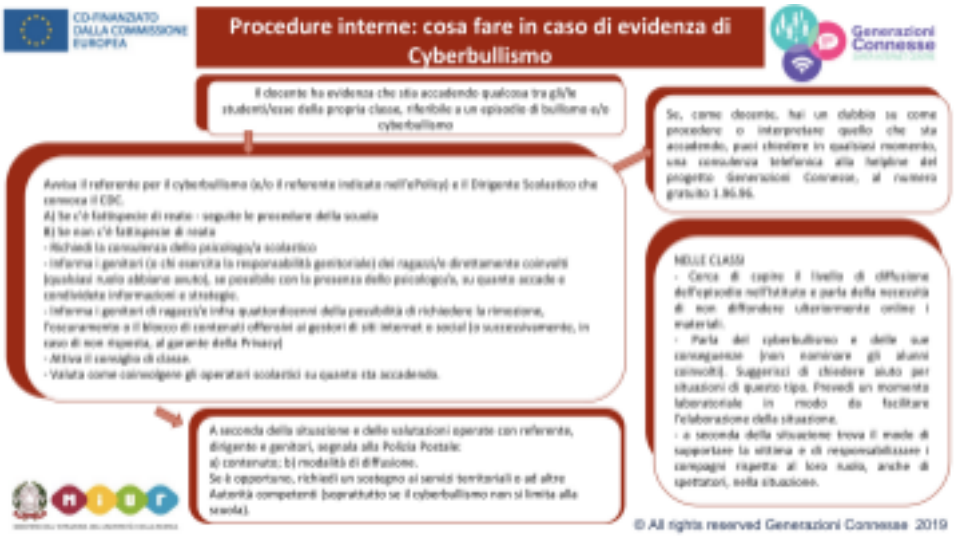
Aziende Sanitarie Locali: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.

Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.

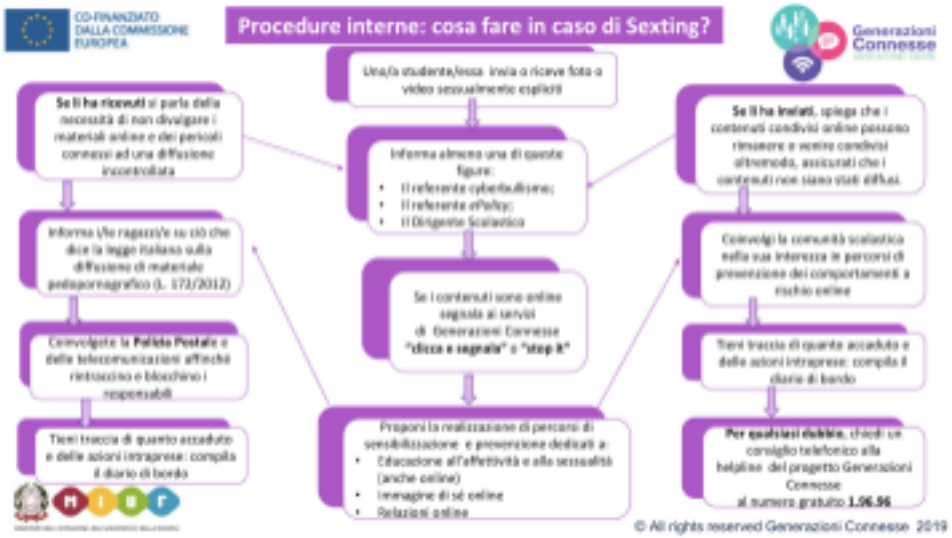
Tribunale per i Minorenni: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

5.4. - Allegati con le procedure

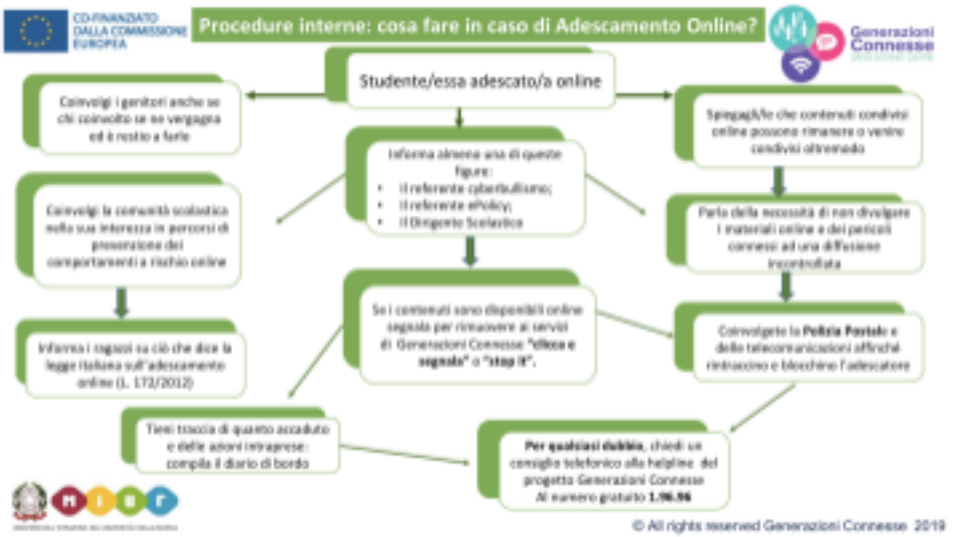
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?



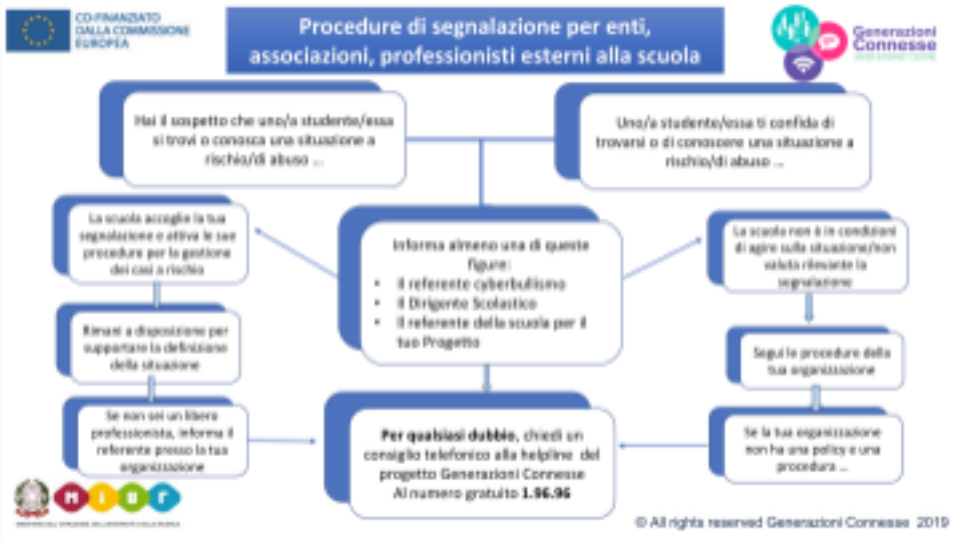
Procedure interne: cosa fare in caso di sexting?



Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Le segnalazioni verranno prese in analisi dai membri del Team Digitale dell'Istituto i quali intratterranno colloqui con gli allievi e le persone coinvolte nell'incidente. Verrà presa visione del materiale digitale relativo al fatto. Si procederà poi alla classificazione dell'incidente secondo le modalità succitate e sarà fatto rapporto dettagliato al Dirigente Scolastico. Quando il caso lo richieda verrà convocata la famiglia dello studente ed eventualmente coinvolte le autorità competenti (vedi Polizia Postale).

Gestione degli incidenti

In questa scuola:

1. Ricevuto il verbale del caso si procede alla registrazione nel registro incidenti

2. Si classifica l'accaduto in infrazione da gestire all'interno della classe/scuola/istituto o da comunicare alle autorità competenti

3 . Viene informato il dirigente scolastico del fatto e delle procedure messe in atto

Modulo per registrare gli incidenti:

https://forms.gle/R3F9GKZ5ZFdnwVr99

• tutto il personale è incoraggiato ad essere vigile nelle questioni di rendicontazione, nella fiducia che i problemi saranno affrontati in modo rapido e

sensibile, attraverso i vari processi che la scuola mette in atto

• è assicurato il supporto delle autorità locali, polizia postale, ecc. per affrontare le questioni di ES e monitoraggio e/o segnalazione degli incidenti di sicurezza

• genitori/ tutori sono specificamente informati degli incidenti che coinvolgono i giovani, per i quali sono responsabili.

• è garantito il contatto con la polizia postale e gli organi competenti ogni qual volta il personale scolastico o gli alunni ricevano comunicazioni on-line ritenute particolarmente preoccupanti o contro la normativa vigente

GESTIONE DEI CASI

COMPORTAMENTO CONSIGLIATO IN CASO DI INCIDENTE INVOLONTARIO.

Chi usa le apparecchiature deve spegnere il monitor o chiudere il laptop. Se dovessero presentarsi dati spiacevoli o spaventosi parlarne subito con un adulto di fiducia: insegnante, membro del Team Digitale.