



UNIONE EUROPEA

FONDI
STRUTTURALI
EUROPEI

pon
2014-2020

PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO-FESR



Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
Direzione Generale per Interventi in materia di edilizia
scolastica, per la gestione dei fondi strutturali per
l'istruzione e per l'innovazione digitale
Ufficio IV

MIUR

Ministero dell'Istruzione, dell'Università e della Ricerca
Istituto Comprensivo di Bellusco e Mezzago
Via Pascoli, 9 - 20882 BELLUSCO (MB)
Tel. 039/623554 - Fax 039/623665
E-mail: segreteria@icbelluscomezzago.it
Miic8cp00e@pec.istruzione.it
C.F. 94030940152

E-Safety Policy

SOMMARIO

1. Introduzione	3
• SCOPO DELLA POLICY	3
• RIFERIMENTI NORMATIVI	3
• INDIVIDUAZIONE AREE DI RISCHIO	4
• RUOLI E RESPONSABILITÀ.....	5
• CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA	7
• GESTIONE DELLE INFRAZIONI ALLA POLICY.....	7
• MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO	8
• INTEGRAZIONE DELLA POLICY CON REGOLAMENTI ESISTENTI.	9
2. Formazione e Curricolo	10
3. Gestione dell'infrastruttura e della strumentazione ICT della scuola.	11
• INTERNET	11
• E-MAIL	11
• BLOG E SITO WEB DELLA SCUOLA	11
• SOCIAL NETWORK E STRUMENTI DI CONDIVISIONE.....	12
4. Strumentazione personale	13
5. Prevenzione, rilevazione e gestione dei casi	13
• PREVENZIONE.....	13
• AZIONI	14
• RILEVAZIONE	15
Allegati	16
Annessi	16

1. INTRODUZIONE

SCOPO DELLA POLICY

La nostra Scuola intende incrementare l'uso delle tecnologie informatiche nella didattica e nell'organizzazione generale della scuola affinché possano essere utilizzate per svolgere esperienze formative e per condurre in modo più efficiente le funzioni amministrative.

Si ritiene importante individuare i principi fondamentali in merito all'utilizzo delle tecnologie per salvaguardare la comunità scolastica nel lavoro in rete e anche per assistere il personale della scuola a lavorare in modo sicuro e responsabile con le tecnologie di comunicazione.

A tal fine bisogna impostare chiare aspettative di comportamento e/o codici di condotta per un uso responsabile a scopo didattico e organizzativo e per affrontare abusi online come ad esempio il cyberbullismo.

Per sviluppare competenza digitale è necessario promuovere una cultura di rispetto di regole comuni nell'uso dei servizi telematici e di regole di buon comportamento (Netiquette) riferite ora anche ai Social Network e alla conoscenza delle condizioni del loro utilizzo.

RIFERIMENTI NORMATIVI

Art. 3-33-34 della Costituzione Italiana

Direttiva MIUR n.16 del 5 febbraio 2007

MIUR aprile 2015 "Linee di orientamento per azioni di prevenzione del bullismo e di contrasto al cyberbullismo"

LEGGE n71/2017 sulla tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo

Legge Regionale 7 febbraio 2017, n. 1 Disciplina degli interventi regionali in materia di prevenzione e contrasto al fenomeno del bullismo e del cyberbullismo

MIUR prot. n. 5515 del 27 ottobre 2017 Aggiornamento LINEE DI ORIENTAMENTO per la prevenzione e il contrasto del cyberbullismo

INDIVIDUAZIONE AREE DI RISCHIO

Le aree di rischio individuabili sono le seguenti.

AREA DEI CONTENUTI

- esposizione a contenuti inappropriati
- visita di siti web inappropriati
- validazione dei contenuti: autenticità delle informazioni
- rispetto del copyright

AREA DELLA COMUNICAZIONE E CONDOTTA

- grooming
- sexting
- reputazione on-line
- bullismo
- bullismo on-line
- furto di identità
- abuso di utilizzo di devices
- dipendenza da videogiochi

RUOLI E RESPONSABILITÀ

Le linee guida sono presenti nel “Regolamento d’uso del laboratorio di informatica, aula video e aule LIM” di Istituto approvato dal Collegio Docenti e dal Consiglio di Istituto. Le modalità con cui viene garantita la sicurezza degli accessi e dei dati sono definite nel documento AgID.

A seguire sono delineati ruoli e responsabilità.

RUOLO	RESPONSABILITÀ
Dirigente Scolastico	<ul style="list-style-type: none">● Assumere la responsabilità generale per la sicurezza dei dati● Garantire l’attuazione di quanto dichiarato nel documento AgID● Assicurare che il personale riceva una formazione adeguata● Essere a conoscenza e attuare le procedure da seguire in caso di infrazione della E-Safety Policy
Responsabile della Sicurezza online (Referente Bullismo e Cyberbullismo)	<ul style="list-style-type: none">● Assicurare che l’educazione alla sicurezza online sia incorporata in tutto il programma di studi● Promuovere la formazione e la consulenza per il personale● Condividere le procedure di segnalazione e/o intervento in caso di bullismo e cyberbullismo
Animatore Digitale e Team	<ul style="list-style-type: none">● Collaborare con le figure tecniche per definire e aggiornare il documento AgID (Animatore Digitale)● Revisionare e aggiornare i regolamenti di utilizzo degli strumenti digitali in uso, quelli relativi alla E-Safety Policy e i curricula digitali di Istituto

<p>Tutto il personale scolastico</p>	<ul style="list-style-type: none"> ● Conoscere le normative che regolano l'utilizzo dei contenuti elettronici ● Utilizzare i dispositivi informatici rispettando le disposizioni vigenti ● Conoscere i problemi di sicurezza connessi ad ogni tipo di device (cellulari, fotocamere, tablet e dispositivi privati...) ● Segnalare al Dirigente qualsiasi sospetto di abuso o problematiche relative alla sicurezza delle TIC ● Usare comportamenti sicuri, responsabili e professionali nell'uso della tecnologia
<p>In particolare, i docenti</p>	<ul style="list-style-type: none"> ● Inserire nella programmazione tematiche legate alla sicurezza online e alle norme di pubblicazione ● Supervisionare e controllare gli alunni durante le attività che prevedono l'utilizzo di tecnologia digitale ● Garantire l'utilizzo di Netiquette nella navigazione online
<p>Gli alunni</p>	<ul style="list-style-type: none"> ● Leggere, comprendere e accettare la E-Safety Policy ● Elaborare informazioni attraverso ricerche online evitando il plagio e rispettando le norme sul diritto d'autore ● Capire l'importanza dell'uso improprio e dell'accesso a materiali inappropriati e segnalarne gli abusi ● Utilizzare la comunicazione online seguendo le regole della Netiquette e porre attenzione alle relazioni e sapere quali azioni intraprendere se si individuano situazioni di

	vulnerabilità e cyberbullismo
I genitori	<ul style="list-style-type: none"> ● Sostenere la scuola nel promuovere la sicurezza online e approvare il suddetto accordo ● Assicurarsi che la scuola abbia preso le precauzioni necessarie circa l'uso corretto della tecnologia da parte degli alunni

CONDIVISIONE E COMUNICAZIONE DELLA POLICY ALL'INTERA COMUNITÀ SCOLASTICA

La E-Safety Policy d'Istituto si applica a tutti i membri della scuola: personale, studenti, genitori, utenti della comunità che ne hanno accesso.

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

- Pubblicazione della E-Safety Policy sul sito della scuola
- Accordo di utilizzo accettabile, discusso con studenti e genitori, all'inizio dell'anno scolastico, tramite il Patto di Corresponsabilità che sarà sottoscritto dalle famiglie e rilasciato alle stesse
- Accordo di utilizzo accettabile rilasciato al personale scolastico

GESTIONE DELLE INFRAZIONI ALLA POLICY

La scuola prenderà tutte le precauzioni necessarie per garantire la sicurezza online (documento AgID).

Tuttavia, a causa della interconnessione su scala internazionale collegata ai contenuti in Internet, la disponibilità di tecnologie mobili e velocità di cambiamento, non è possibile garantire che il materiale non idoneo apparirà mai su un computer della scuola o dispositivo mobile. Né la scuola, né l'autorità locale possono accettare la responsabilità per il materiale accessibile o le conseguenze di accesso ad Internet.

Tramite comunicazione da parte dei docenti del "Regolamento d'uso del laboratorio di informatica, aula video e aule LIM", il personale e gli alunni riceveranno informazioni sulle infrazioni in merito a:

- scaricare file video-musicali protetti da copyright o attraverso siti poco sicuri
- visitare siti non necessari per attività didattica
- navigare in siti non accettati dalla protezione interna della scuola

- alterare i parametri di protezione dei computer
- utilizzo della rete per interessi privati o che esulano dalla didattica
- rispetto delle norme sui diritti di autore

Tramite curriculare attività didattica nelle classi e con l'ausilio di progetti con esperti esterni docenti e alunni saranno formati in merito ai rischi dell'utilizzo improprio di Internet e di dispositivi connessi:

- violazione della privacy
- web-reputation
- grooming
- sexting
- furto di identità
- cyberbullismo
- utilizzo eccessivo di devices
- dipendenza da videogiochi
- esposizione a contenuti lesivi della salute fisica e mentale

Saranno altresì comunicate le eventuali sanzioni applicabili alla violazione da applicarsi a seconda della gravità dell'infrazione:

- Informare il docente coordinatore di classe
- Informare il Dirigente Scolastico e il docente responsabile della sicurezza online
- Informare i genitori o i tutori
- Il ritiro del cellulare fino a fine giornata
- La rimozione di Internet o del computer di accesso per un periodo
- Comunicazione alle autorità competenti

Il docente responsabile della sicurezza online fungerà da primo punto di contatto per qualsiasi reclamo. Qualsiasi lamentela personale di abuso sarà riferita al Dirigente Scolastico

Le denunce di cyberbullismo saranno trattate secondo in conformità con la legge attuale e le procedure di protezione dell'infanzia.

MONITORAGGIO DELL'IMPLEMENTAZIONE DELLA POLICY E SUO AGGIORNAMENTO

La E-Safety Policy sarà riesaminata annualmente o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e tutte le modifiche della Policy saranno discusse in dettaglio con tutti i membri del personale docente e saranno integrate con quanto definito nel "Regolamento d'uso del laboratorio di informatica, aula video e aule LIM" e nel Documento AgID.

Nell'ambito del monitoraggio dell'implementazione della E-Safety Policy si terranno in considerazione i dati annuali sulla base del seguente documento:

ANNO a.s...../.....	NUMERO DI SEGNALAZIONI	NUMERO DI INFRAZIONI	NUMERO DI SANZIONI DISCIPLINARI

INTEGRAZIONE DELLA POLICY CON REGOLAMENTI ESISTENTI.

La presente E-Policy si integra con:

- "Regolamento d'uso del laboratorio di informatica, aula video e aule LIM"
- Documento di Misure minime di sicurezza ICT per le pubbliche amministrazioni

2. FORMAZIONE E CURRICOLO

CURRICOLO SULLE COMPETENZE DIGITALI PER GLI STUDENTI

Si vedano i curricula di Istituto

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

Si veda il Piano di Aggiornamento del PTOF

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

Vedi piano di aggiornamento di Istituto.

SENSIBILIZZAZIONE DELLE FAMIGLIE

Nelle assemblee di classe saranno presentati alle famiglie i curricula sulle competenze digitali e le modalità di attuazione nelle singole classi.

L'Istituto prevede occasioni di formazione e sensibilizzazione alle tematiche affrontate dall'E-policy rivolti alle famiglie, tra cui:

- Organizzare incontri di approfondimento con esperti
- Distribuire volantini e pubblicazioni sul sito della scuola
- Diffondere iniziative promosse dalle reti territoriali
- Promuovere il ricorso a siti nazionali di sostegno quali il sito www.generazioniconnesse.it

3. GESTIONE DELL'INFRASTRUTTURA E DELLA STRUMENTAZIONE ICT DELLA SCUOLA.

INTERNET

I seguenti punti sono definiti Documento di Misure minime di sicurezza ICT per le pubbliche amministrazioni:

- Accesso ad Internet (filtri antivirus e navigazione)
- Gestione accessi (password, backup, ecc.)

E-MAIL

Sui dispositivi della scuola, la consultazione e invio di mail da parte di docenti e personale della scuola è consentito solo per esigenze di servizio.

Tale utilizzo avviene solo tramite accesso ai propri indirizzi personali o tramite l'utilizzo dell'indirizzo di posta del plesso di appartenenza, senza utilizzo di software di gestione della posta installato nel singolo dispositivo.

È cura del docente uscire dalla pagina mail online.

BLOG E SITO WEB DELLA SCUOLA

Il Dirigente Scolastico e il personale incaricato di gestire le pagine del sito della Scuola hanno la responsabilità di garantire che il contenuto pubblicato sia accurato e appropriato.

La scuola offre all'interno del proprio sito una serie di servizi alle famiglie e ai fruitori esterni.

I docenti che desiderano pubblicare attività didattiche dovranno seguire la procedura che sarà definita dal Dirigente.

Per il sito la mail viene richiesta a chi si iscrive che diventa utente, ciò è possibile solo per il personale scolastico.

La mail viene usata in automatico da WordPress che invia link di conferma iscrizione.

L'iscrizione è riservata solo ed esclusivamente al personale della scuola.

Solo l'applicato di segreteria incaricato può consultare e modificare gli indirizzi mail.

Per quanto concerne la Privacy Policy si fa riferimento a quanto scritto nel seguente link <https://icsbelluscomezzago.it/amministrazione-digitale/privacy/> .

I Blog di plesso o classe che sono attivati devono rispettare le disposizioni sulla tutela della privacy e del copyright.

Le immagini e i filmati costituiscono dati personali o fonti di rinvenimento di dati personali degli alunni.

Non è consentito pubblicare né foto di minori riconoscibili, anche tramite ingrandimenti, né informazioni che ne consentano il riconoscimento o l'utilizzo da parte di terzi.

Tali disposizioni sono riferite anche ad eventi organizzati dalla scuola stessa.

Non è consentita la pubblicazione di immagini con riferimenti sessuali o fomentanti violenza e razzismo.

È consentito ai docenti la pubblicazione di blog a scopi didattici e di comunicazione e collaborazione con le famiglie. Le famiglie ne devono essere informate ed è affidata a esse la sorveglianza durante l'accesso al blog da casa.

SOCIAL NETWORK E STRUMENTI DI CONDIVISIONE

Non è consentito l'utilizzo di Facebook da parte degli alunni.

La condivisione di contenuti e materiali con gli alunni deve avvenire attraverso i canali predisposti dalla scuola e piattaforme che garantiscano la tutela degli alunni.

Se richiesta l'iscrizione da parte degli alunni essa deve avvenire tramite nickname senza inserimento di dati personali e sensibili dell'alunno.

Qualora sia richiesta iscrizione dell'alunno tramite indirizzo Mail, previa autorizzazione, essa avverrà con mail di uno dei genitori.

Nell'utilizzo di social network, strumenti di condivisione si ribadisce che:

- non è consentito pubblicare né foto di minori riconoscibili, anche tramite ingrandimenti, né informazioni che ne consentano il riconoscimento o l'utilizzo da parte di terzi
- non è consentita la pubblicazione di immagini con riferimenti sessuali o fomentanti violenza e razzismo
- non sono consentiti commenti che ledano la persona
- non sono ammessi commenti riferibili ad atteggiamenti di prevaricazione e bullismo.

4. STRUMENTAZIONE PERSONALE

Se inserito in progettazione didattica, agli studenti è consentito l'utilizzo di cellulare, tablet ecc., sotto la sorveglianza dell'insegnante e per ragioni prettamente scolastiche.

Tutto il personale è autorizzato all'utilizzo di strumenti personali, quali cellulari, tablet ecc., in orario di servizio unicamente per fini didattici, legati alle proprie mansioni di servizio e per la compilazione del registro elettronico solo qualora non sia possibile accedervi coi mezzi messi a disposizione della scuola.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

PREVENZIONE

La scuola intende favorire l'utilizzo del digitale come strumento di espressione della libertà di espressione e comunicazione con famiglie e alunni, pertanto è consentita l'espressione di pareri discordanti o di mancato gradimento.

Vengono invece considerati abusi meritevoli di segnalazione i contenuti palesemente impropri o illeciti.

È fatto obbligo al docente che utilizzi a scopo didattico, la navigazione nei Social e le applicazioni Web di informarsi in merito ai diritti e doveri dell'utente, al regolamento.

La pubblicazione di contenuti, foto, video deve rispettare la normativa in merito ai diritti d'autore e le seguenti disposizioni.

Non è consentito:

- pubblicare né foto di minori riconoscibili, anche tramite ingrandimenti, né informazioni che ne consentano il riconoscimento o l'utilizzo da parte di terzi;
- pubblicare di immagini con riferimenti sessuali o fomentanti violenza e razzismo;
- commenti che ledano la dignità della persona;
- commenti riferibili ad atteggiamenti di prevaricazione e bullismo.

La scuola si propone di tenere un monitoraggio aggiornato delle segnalazioni.

Si impegna a predisporre e proporre interventi di consulenza e supporto se richiesti o relativamente ai casi più gravi.

La scuola, affianca la famiglia, nella prevenzione di comportamenti a rischio attraverso le seguenti azioni:

- Educazione all'affettività e all'empatia;
- Creare un clima di solidarietà
- Combattere l'indifferenza e la deresponsabilizzazione morale
- Incoraggiare le vittime a chiedere aiuto
- Sottrarre al (cyber)bullo potenziali proseliti.
- Proporre attività didattica che comporti l'utilizzo di tecnologie;
- Informare gli alunni sui rischi presenti in Rete, senza demonizzarla, ma sollecitandone un utilizzo consapevole;
- Educare alla prudenza nel fornire dati e informazioni personali, alla riservatezza di password, ad abbandonare un sito dai contenuti che possono turbare o spaventare e a non incontrare persone conosciute in Rete senza averne prima parlato coi genitori
- Mostrare come usare e valutare in modo critico ciò che incontrano durante la navigazione in rete
- Informare su quali siano i comportamenti illeciti in Rete
- Predisporre e controllare le strumentazioni a disposizione della scuola per impedire l'accesso o eliminare contenuti ritenuti non idonei

AZIONI

Qualora un utente commetta involontariamente un abuso o un errore, pubblicando del materiale illecito, non idoneo o offensivo, è necessario contattarlo e metterlo al corrente delle regole in uso.

I docenti sono tenuti a prevedere per gli alunni, in ogni anno scolastico, percorsi educativo-didattici di educazione all'utilizzo consapevole degli strumenti multimediali e della rete e ai rischi connessi al loro uso improprio.

Per cui è necessario cogliere i segnali che i ragazzi ci lanciano quando si trovano in una situazione di disagio o di difficoltà

Sono tenuti a cogliere i segnali che i ragazzi manifestano se si trovano in situazioni di disagio e difficoltà e che possano evolvere in atti di bullismo/cyberbullismo riferiti a tutte le componenti in gioco (vittime, bulli, spettatori). A seguito dell'osservazione sono altresì tenuti a intervenire in modo educativo e non punitivo, agendo in primis sul creare un clima solidale nella classe.

Le famiglie sono chiamate a collaborare sia educando i propri figli sia vigilando sui loro comportamenti.

Saranno utilizzate tutte le risorse offerte dal territorio per promuovere approfondimenti e formazione sull'utilizzo dei TIC e sulla conoscenza dei fenomeni del bullismo e cyberbullismo.

RILEVAZIONE

Cosa segnalare

- Offese e insulti tramite messaggi di testo, e-mail, pubblicati su social network o tramite telefoni;
- Diffusione di foto o video che ritraggono situazioni intime, violente o spiacevoli tramite il cellulare, siti web o social network;
- Esclusione dalla comunicazione on-line, dai gruppi;
- Furto, appropriazione, uso e rivelazione ad altri di informazioni personali come le credenziali d'accesso all'account e-mail, social network, ecc.
- Segnali di dipendenza da device e videogiochi

Come segnalare: quali strumenti e a chi

Gli alunni stessi potranno segnalare situazioni di difficoltà come segue:

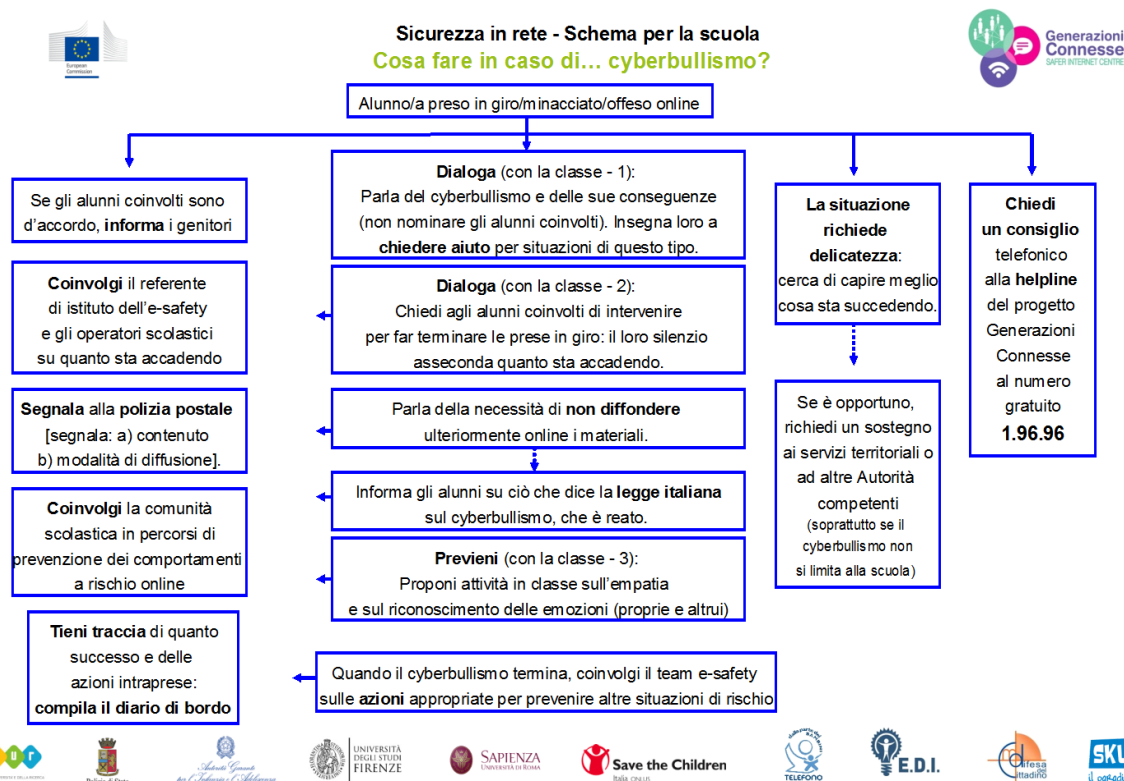
- collocazione in alcuni punti delle scuole secondarie di “bully-boxes” (cassette in cui gli studenti anonimamente potranno segnalare le proprie preoccupazioni o esperienze, scrivendole e imbucandole)
- colloquio col un docente
- richiesta di colloquio con Dirigente Scolastica

I docenti, all'interno di ogni Consiglio di classe, sono tenuti a tenere traccia delle situazioni di rischio osservate e degli episodi di bullismo e/o cyberbullismo rilevati, informando Dirigente Scolastico e referente del Bullismo e Cyberbullismo.

Come gestire le segnalazioni

Le tappe da seguire quando si presenta un caso di (cyber)bullismo sono:

- fermare immediatamente l'abuso;
- dare sostegno alla vittima;
- lavorare sul gruppo classe affinché riconosca la gravità dell'accaduto e la propria partecipazione attraverso il silenzio o forme blande di coinvolgimento;
- lavorare sul gruppo classe col fine di creare un clima di solidarietà, combattere l'indifferenza e la deresponsabilizzazione morale, incoraggiare le vittime a chiedere aiuto, sottrarre al (cyber)bullo potenziali proseliti
- dare supporto al bullo con un programma educativo che si focalizzi su due fronti il coinvolgimento attivo del gruppo dei pari per sviluppare l'empatia e l'intervento dei docenti per gestire l'aggressività e la rabbia.



ALLEGATI

1. “Regolamento d’uso del laboratorio di informatica, aula video e aule LIM”
2. Documento di Misure minime di sicurezza ICT per le pubbliche amministrazioni
3. Patto di corresponsabilità

ANNESI

1. Procedure operative per la gestione delle infrazioni alla Policy
2. Modello monitoraggio annuale infrazioni alla E-Safety Policy