ISTITUTO COMPRENSIVO
"GIUSEPPE TALIERCIO"
Via Commercio, 1 MARINA DI CARRARA
(MS)
tel. 0585/788353 fax 0585/788372
C.F.91019490456 – codice univoco: UF61Y1

msic815001@pec.istruzione.it
msic815001@istruzione.it
www.comprensivotaliercio.edu.it

E-Safety Policy IC Taliercio

1. Introduzione
Scopo della Policy.
Ruoli e Responsabilità
Informativa per i soggetti esterni che erogano attività educative nell'Istituto
Condivisione e comunicazione della Policy all'intera comunità scolastica.
Gestione delle infrazioni alla Policy.
Monitoraggio dell'implementazione della Policy e suo aggiornamento.
Integrazione della Policy con Regolamenti esistenti.

2. Formazione e Curricolo
Curricolo sulle competenze digitali per gli studenti.
Formazione dei docenti sull'utilizzo e l'integrazione delle TIC nella didattica.
Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
Sensibilizzazione delle famiglie.

3. Gestione dell'infrastruttura e della strumentazione ICT della scuola.
Accesso ad internet:
Gestione accessi
E-mail.
Sito web della scuola
Social network.
Cloud storage
Registro elettronico
Protezione dei dati personali.

4. Strumentazione personale
Per gli studenti:
Per i docenti:
Per il personale della scuola:

5. Prevenzione e rilevazione dei casi
Cyberbullismo
Hate speech
Dipendenza da Internet e gioco online
Sexting
Adescamento online
Pedopornografia

6. **Segnalazione e gestione dei casi**
Strumenti a disposizione di studenti e studentesse

1. INTRODUZIONE

- **Scopo della Policy**

L'Istituto Comprensivo Taliercio ha aderito al progetto Generazioni Connesse, S.I.C. (Safer Internet Center), promosso dal MIUR, in collaborazione con la Comunità Europea. In conformità con quanto proposto dal progetto e con le LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo la nostra scuola ha elaborato questo documento per delineare una propria linea di condotta nei confronti dell'utilizzo delle tecnologie dell'informazione e delle comunicazioni nella didattica, in ambito scolastico ed anche extrascolastico, particolarmente in riferimento ad attività di studio domestico. Il documento sarà revisionato e integrato annualmente

Questa *Policy* si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici dell'Istituto Comprensivo Taliercio.
In particolare l'intento della scuola è quello di promuovere l'uso consapevole e critico da parte degli alunni delle tecnologie digitali e di internet, di far acquisire loro procedure e competenze "tecniche" ma anche corrette norme comportamentali, di prevenire ovvero rilevare e fronteggiare le problematiche che derivano da un utilizzo non responsabile, pericoloso o dannoso, delle tecnologie digitali.

- **Ruoli e Responsabilità (che cosa ci si aspetta da tutti gli attori della Comunità Scolastica)**

Gli adulti hanno un ruolo fondamentale nel garantire che bambini e adolescenti siano in grado di utilizzare le tecnologie digitali e che lo facciano in modo appropriato e sicuro, ruolo che vede coinvolti a pieno titolo tutti coloro che hanno un ruolo educativo, oltre che formativo, primi fra tutti i genitori e la comunità scolastica nel suo complesso.
Non va tuttavia sottovalutato il ruolo degli studenti come primi attori del percorso di acquisizione della capacità di positiva gestione delle proprie competenze digitali: in tale ottica si rende indispensabile responsabilizzare e rendere attivi gli studenti nell'uso delle TIC.

1) Il Dirigente scolastico nel promuovere l'uso consapevole delle tecnologie e di internet
● cura la sicurezza on-line della comunità scolastica;
● favorisce la cultura dell'inclusione dell'altro/a e delle differenze, e l'utilizzo positivo e responsabile delle Tecnologie dell'Informazione e della Comunicazione (TIC) , tramite incontri con il personale e la promozione/adesione a percorsi formativi e di autoformazione del personale docente, l'attivazione di progettualità dedicate per gli alunni.

2) Il Direttore dei servizi generali e amministrativi
● assicura, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni

● garantisce il funzionamento dei diversi canali di comunicazione della scuola (circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente Scolastico nell'ambito dell'utilizzo delle tecnologie digitali e di internet;

3) Animatore Digitale e Team dell'Innovazione
● Promuovono l'aggiornamento dei docenti

● Propongono e promuovono l'uso delle TIC
● Hanno il compito di assicurare che l'e-Safety sia a conoscenza di tutto il personale;
● fornisce al personale, agli alunni e ai genitori consulenza e informazioni in relazione ai rischi on line e alle misure di prevenzione e gestione degli stessi;
● riceve segnalazioni di incidenti e-Safety *e crea un registro degli incidenti* e informa il DS o Collaboratori

4) Docente Funzione strumentale per le nuove tecnologie
● cura la parte didattica del sito web della scuola;
● supporta l'attività laboratoriale con consigli, aiuti e chiarimenti;
● assicura , per quanto è nelle sue possibilità, che il personale possa accedere alla rete della scuola solo tramite password;

5) Docenti:
● illustrano ai propri allievi le regole di utilizzo contenute nel presente documento;
● danno chiare indicazioni sul corretto utilizzo della strumentazione multimediale, di internet, ecc.;
● segnalano prontamente eventuali malfunzionamenti o danneggiamenti al docente funzione strumentale;
● non divulgano le credenziali di accesso alla rete wifi;
● non salvano sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;
● si informano/si aggiornano sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
● garantiscono che gli alunni capiscano e seguano le regole per prevenire e contrastare l'utilizzo scorretto e pericoloso delle TIC e di internet;
● controllano l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito);
● nelle lezioni in cui è programmato l'utilizzo di Internet, guidano gli alunni a siti controllati e verificati come adatti per il loro uso e controllano che nelle ricerche su Internet siano trovati e trattati solo materiali idonei;
● segnalano al Dirigente Scolastico e ai genitori qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.

6) Il Personale ATA è tenuto a:
● avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
● aver letto, compreso e sottoscritto la presente policy;
● segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o ai suoi collaboratori o alla Funzione Strumentale per le nuove tecnologie o all'Animatore Digitale per le opportune indagini / azioni / sanzioni;

7) Gli studenti devono:
● utilizzare le TIC solo su indicazioni del docente;
● in caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate comunicarlo immediatamente all'insegnante;
● non eseguire tentativi di modifica della configurazione di sistema delle macchine;
● non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
● non utilizzare propri dispositivi esterni personali senza aver acquisito il permesso da parte dell'insegnante;
● chiudere correttamente la propria sessione di lavoro;

● essere consapevoli dei problemi di sicurezza connessi con l'uso di telefoni cellulari, telecamere e dispositivi portatili;
● essere responsabili dell'utilizzo delle attrezzature tecnologiche della scuola e comprendere l'importanza di adottare buone pratiche di e-Safety anche quando utilizzano tecnologie digitali fuori dalla scuola

7) I genitori hanno i seguenti compiti:
● sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle Tecnologie dell'Informazione e delle Comunicazioni nella didattica;
● seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti, in particolare controllare l'utilizzo del pc e di internet;
● concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di internet;
● fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e del telefonino in generale.

-
-

- **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 di 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).

- Condivisione e comunicazione della *policy* all'intera comunità scolastica.

Il presente documento sarà oggetto di condivisione e revisione da parte dell'intera comunità scolastica con il coinvolgimento di studenti, docenti e famiglie, con l'approvazione degli organi collegiali. 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 scolastco ed è pubblicato sul diario scolastico degli alunni
Per evitare che l'adozione di questa *policy* rappresenti un mero atto formale, l'Istituto si impegna a prendere spunto da essa come base di partenza per una serie di azioni e iniziative. A partire dalla pubblicazione sul sito della scuola, si possono ipotizzare per esempio:
- per il corpo docente un confronto collegiale, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla *policy* vigente ed elaborazione di protocolli condivisi di intervento;
- per gli alunni, la discussione in classe della *policy* nei primi giorni di scuola, con particolare riguardo alle nuove classi prime;
- per i genitori, l'organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare.

- Gestione delle infrazioni della *policy*.
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.

- Monitoraggio dell'implementazione della Policy e suo aggiornamento

Il monitoraggio dell'implementazione della Policy verrà curata dal DS in collaborazione con l'Animatore Digitale e il Team dell'Innovazione che promuoveranno inoltre gli eventuali aggiornamenti che si rendano opportuni. ~~secondo una logica di condivisione con tutto il corpo docente e le famiglie.~~ Le modifiche del documento saranno discusse con tutti i membri del personale docente.

- Integrazione della Policy con documenti esistenti

Il presente documento si integra pienamente con obiettivi e contenuti dei seguenti documenti: PTOF incluso il piano per l'attuazione del PNSD , PTOF, Regolamento d'Istituto, Patto Educativo di corresponsabilità, Regolamento LIM, Protocollo bullismo, Didattica a distanza linee guida per gli alunni.
"Linee di orientamento Contro il bullismo e il cyberbullismo" (MIUR 13 Aprile 2015)
"Piano Nazionale per la prevenzione del bullismo e del cyberbullismo a scuola
(MIUR 2016/2017).
"Legge n. 71 del 29/05/2017, Disposizioni a tutela dei minori per la prevenzione del fenomeno del cyberbullismo".

2. FORMAZIONE E CURRICOLO

- Curricolo sulle competenze digitali per gli studenti

La raccomandazione 2006/962/CE del Parlamento Europeo e del Consiglio dell'Unione Europea individua il quadro di riferimento europeo in materia di competenze chiave per l'apprendimento permanente. Tra queste è citata la competenza digitale, ovvero il "saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) per il lavoro, il tempo libero e la comunicazione".
Al fine di promuovere l'acquisizione e l'incremento delle competenze digitali, verranno svolte attività dirette a perseguire i seguenti obiettivi:

1. conoscere e acquisire consapevolezza su natura, ruolo e opportunità delle TSI nella vita quotidiana e professionale;

2. distinguere il reale dal virtuale e riconoscerne le correlazioni e le conseguenze delle correlazioni;

3. sviluppare le abilità di base nelle TSI (saper usare il computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni);

4. usare le informazioni in modo critico, accertandone la provenienza e l'affidabilità;

5. acquisire consapevolezza su come le TSI possono coadiuvare la creatività e l'innovazione;

6. riflettere sulle problematiche legate alla validità e all'affidabilità delle informazioni disponibili;
7. acquisire consapevolezza sulle opportunità e sui potenziali rischi di Internet e della comunicazione tramite i supporti elettronici;

8. riflettere sui principi giuridici ed etici di base che si pongono nell'uso interattivo delle TSI (netiquette, privacy…).

In virtù della valenza trasversale delle competenze digitali, la loro acquisizione è promossa attraverso percorsi didattici disciplinari e/o interdisciplinari inerenti diverse aree, coerentemente con gli obiettivi individuati nel Curricolo di Istituto e nelle programmazioni individuali.

- Formazione dei docenti sull'utilizzo e l'integrazione delle TIC 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.
Molti docenti dell'istituto nel corso degli anni hanno partecipato a corsi di formazione nell'ambito del piano nazionale scuola digitale organizzati nella provincia e dal nostro Istituto, sono inoltre disponibili ad aggiornarsi per mantenere al passo la propria formazione, in rapporto all'utilizzo di metodologie innovative di insegnamento e apprendimento e all'eventuale ricorso alla didattica a distanza.
Il percorso complesso della formazione specifica dei docenti sull'utilizzo delle TIC nella didattica, non esauribile nell'arco di un anno scolastico, può pertanto prevedere momenti di autoaggiornamento, momenti di formazione personale o collettiva anche all'interno dell'istituto, con la condivisione delle conoscenze dei singoli e il supporto dell'Animatore Digitale, la partecipazione alle iniziative promosse dall'Amministrazione centrale e dalle scuole polo e a corsi di aggiornamento online.

- 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, referenti 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.

I docenti hanno partecipato al corso di formazione legato al progetto "Generazioni connesse" e si sono organizzati incontri di formazione sull' uso responsabile e sicuro delle nuove tecnologie, in particolare di internet (accesso a facebook e social network in genere da parte dei minori, rispetto delle regole nel mondo virtuale della rete ecc.) con agenti della Polizia Postale. Tali incontri sono stati aperti anche a i genitori

- Sensibilizzazione delle famiglie

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.

Come detto al paragrafo precedente, dall'a.s. 2012/13 sono organizzati incontri di formazione sull' uso responsabile e sicuro delle nuove tecnologie con agenti della Polizia postale, aperti anche ai genitori.

La scuola si impegna alla diffusione delle informazioni e delle procedure contenute nel documento (Policy e-safety) per portare a conoscenza delle famiglie il regolamento sull'utilizzo delle nuove tecnologie all'interno dell'istituto e prevenire i rischi legati a un utilizzo non corretto di internet.

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

L'infrastruttura e la strumentazione ICT dell'Istituto sono un patrimonio di tutti, esse vanno utilizzate nel rispetto delle norme contenute nel " Regolamento di utilizzo delle LIM". I danni causati alle attrezzature saranno a carico di chiunque disattenda il suddetto Regolamento.

L'accesso ad infrastrutture strumentazione ICT utilizzabili per la didattica è riservato agli insegnanti e agli alunni ed è limitato al perseguimento di scopi formativi. I docenti devono formare i propri alunni al rispetto del suddetto Regolamento, per gli aspetti di loro pertinenza.

L'Istituto è dotato di una rete wireless nei plessi della scuola secondaria e della scuola primaria.

Accesso a internet e navigazione

L'accesso a internet è consentito a scopi didattici al personale docente attraverso l'assegnazione di una password comune a tutti. Agli alunni è permessa la navigazione in internet dai tablet e dai notebook o delle aule collegate alle LIM esclusivamente sotto il diretto controllo dei docenti che non devono mai comunicare la password di accesso.

E-mail

L'account di posta elettronica istituzionale è quello fornito dal Ministero dell'Istruzione dell'Università e della Ricerca, sia nella versione posta ordinaria che certificata. Questi account sono utilizzati ordinariamente dagli uffici amministrativi, sia per la posta in ingresso che in uscita: l'invio o ricevimento di posta a scopi didattici avviene su autorizzazione del DS e operativamente è svolto dall'assistente amministrativo addetto.

Da quest'anno durante il periodo della Dad è stata attivata la piattaforma Google Suite for Education, per cui tutti i docenti e gli studenti possiedono l'account di posta elettronica @comprensivotaliercio.edu.it per mezzo del quale possono comunicare.

Sito web della scuola.

La scuola attualmente ha un sito web.

Tutti i contenuti del settore didattico sono pubblicati direttamente dalla funzione strumentale Comunicazione, linguaggi,TIC, che ne valuta con il Dirigente Scolastico la sicurezza e l'adeguatezza .

Social network.
Sono presenti sulla piattaforma Facebook un gruppo chiuso " Dida digiTALI" a cui accedono solo i docenti dell'istituto e una pagina "Istituto Comprensivo Taliercio" curata da alcuni docenti.
Da qualche anno alcune classi della scuola secondaria usano la piattaforma Edmodo per la condivisione di contenuti didattici con studenti della classe e docenti, Da quest'anno con l'avvento della DAD la scuola ha aderito a G.Suite for Education per cui tutte le classi di scuola primaria e secondaria hanno la possibilità di utilizzare gli strumenti offerti dalla piattaforma, tra cui Classroom.

Cloud storage
I docenti si avvalgono di alcuni software di cloud storage per condividere materiale didattico (Dropbox, Google drive).

Registro elettronico.
Ogni famiglia riceve le credenziali per l'accesso riservato al registro elettronico, in cui il corpo docente registra assenze, valutazioni, note e osservazioni. Tramite le stesse credenziali i genitori possono leggere le schede di valutazione di fine quadrimestre dei propri figli: coloro che non possono accedere a Internet e di conseguenza non possono consultare il registro elettronico possono rivolgersi alla segreteria didattica per stampare i documenti di valutazione di fine quadrimestre

Protezione dei dati personali.

Il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Tutto il personale incaricato riceve poi istruzioni particolareggiate applicabili al trattamento di dati personali su supporto cartaceo e su supporto informatico, ai fini della protezione e sicurezza degli stessi.
Viene inoltre fornita ai genitori informativa e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori.
All'atto dell'iscrizione è richiesto alle famiglie di firmare un'autorizzazione scritta per consentire l'uso didattico di immagini e video delle/dei minori per la documentazione delle attività didattiche

4. STRUMENTAZIONE PERSONALE

Per gli alunni

I telefoni cellulari, i tablet e le relative fotocamere e registratori vocali non verranno utilizzati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate e con il permesso dei docenti.

Nella scuola primaria si chiede alle famiglie di non lasciare tali dispositivi ad alunne e alunni; nella scuola secondaria di primo grado sarà permesso agli studenti di portare il telefono cellulare (o altro dispositivo equivalente) a scuola solo previa liberatoria firmata dai genitori (linK al documento). Tale dispositivo dovrà essere spento prima di entrare nell'edificio scolastico e all'ingresso in aula verrà depositato dallo studente dentro un cassetto della cattedra o in una scatola presente in classe e recuperato al termine delle lezioni.

In caso di violazione delle suddette disposizioni, sarà previsto il ritiro temporaneo dei dispositivi da parte del docente che rileva la violazione. Gli strumenti sequestrati saranno consegnati al DS o ai suoi collaboratori e depositati nella cassaforte della segreteria o del plesso e successivamente consegnati al genitore/tutore tempestivamente convocato, che sarà contestualmente informato dell'eventuale sanzione disciplinare comminata al trasgressore.

In caso di uso non consentito del cellulare (o altro dispositivo equivalente) verranno applicati i PROVVEDIMENTI DISCIPLINARI SPECIFICI previsti dal Regolamento disciplinare d'Istituto.

Gli alunni con BES concorderanno con il consiglio di Classe le modalità di un eventuale impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia.

Ai sensi della Direttiva Ministeriale n. 30 del 15 marzo 2007, con la condivisione della presente Policy, "le famiglie si assumono l'impegno di rispondere direttamente dell'operato dei propri figli nel caso in cui, ad esempio, gli stessi arrechino danni ad altre persone" a seguito di violazioni della presente Policy.

Nel caso in cui gli alunni debbano comunicare con la famiglia durante l'orario scolastico, possono usare gratuitamente la linea fissa della scuola autorizzati dai docenti; allo stesso modo le famiglie devono chiamare il centralino della scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

L'invio di materiali abusivi, offensivi o inappropriati è vietato, anche se avviene all'interno di cerchie o gruppi di discussione privati.

Per il personale docente/ATA.

Il personale preferirà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, tablet…); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. I docenti sono autorizzati ad utilizzare devices (tablet e notebook) personali in classe unicamente per fini didattici e professionali. In tal caso la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente al proprietario.

Telefoni cellulari, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate.

La password di accesso alla rete wireless va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni).

Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (floppy disk, chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.
Tutto il personale scolastico è autorizzato ad utilizzare devices personali laddove non stia assolvendo ad un ruolo didattico, a condizione che l'utilizzo non intralci il normale svolgimento delle attività scolastiche, né distragga dal corretto svolgimento delle proprie mansioni. In tal caso la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente al proprietario.
Nell'invitare tutta la comunità scolastica (studenti, docenti, personale ATA e famiglie) ad evitare, per quanto non necessario, la pubblicazione in rete di immagini e/o video ripresi all'interno dell'Istituto (fatta salva la pubblicazione a scopi didattici, previa informativa al Dirigente Scolastico), è bene ricordare che, secondo la normativa vigente, non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese e che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere in gravi violazioni, incorrendo in sanzioni disciplinari, pecuniarie ed eventuali reati.

5. PREVENZIONE E RILEVAZIONE DEI CASI

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.

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.*

- Cyberbullismo
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.

Hate speech

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.
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.

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.

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).

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 genitorie 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 istituto ha già messo in atto il coinvolgimento della comunità scolastica in percorsi di prevenzione dei comportamenti a rischio online anche attraverso giornate dedicate (Internet Day, Giornata della legalità) uso del materiale fornito dalla piattaforma Generazioni Connesse e dal sito Parole Ostili, incontri con la Polizia postale e con personale specializzato di Telefono Azzurro, attività di peer education.
Questi interventi sono tesi a far conoscere e sensibilizzare gli alunni verso un uso responsabile e consapevole della rete, al fine di assicurare loro il rispetto del diritto ad essere tutelati da abusi e violenze da un lato e, allo stesso tempo, suscitare atteggiamenti di rispetto nei confronti degli altri utenti. Le nuove tecnologie si pongono quale strumento attraverso cui sviluppare pratiche di collaborazione tra gli studenti per riconoscere e accettare la diversità e favorire la partecipazione finalizzata alla costruzione dei diversi percorsi formativi a cui sono chiamati tutti gli alunni

6.SEGNALAZIONE E GESTIONE DEI CASI

Gli eventuali casi rilevati verranno gestiti affrontando il problema sotto diversi punti di vista. In primo luogo si informeranno gli alunni sulle conseguenze relative al fenomeno emerso, dall'altro si cercherà di aiutare l'alunno/a coinvolto e vittima creando situazioni il dialogo che consentano di far emergere gli aspetti di criticità per i quali attraverso un confronto si potrà intervenire.
La gestione dei casi rilevati avverrà secondo i protocolli allegati messi a disposizione dalla piattaforma "Generazioni Connesse". **Per quanto riguarda gli episodi di bullismo e cyberbullismo la scuola seguirà Il protocollo apposito, già presente.**
I docenti avranno anche a disposizione uno strumento di rilevamento delle criticità, sul quale descrivere le situazioni che si vengono a determinare, indicando anche le azioni messe in atto.
Inoltre, si potranno avvalere avvalere del servizio Hotline che 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 Center sono il "Clicca e Segnala" di Telefono Azzurro e "STOP-IT" di Save the Children. Una volta ricevuta la segnalazione, gli operatori procederanno a coinvolgere le autorità competenti in materia.

Strumenti a disposizione di studenti e studentesse

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:

scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
docenti referenti per le segnalazioni. (1 per ogni plesso primaria, 2 per la secondaria)

Anche studenti e studentesse, inoltre, possono rivolgersi alla Helpline del progetto Generazioni Connesse, al numero gratuito 1.96.96.

Il nostro piano d'azione per prossimo triennio

Si rende necessario per attuare le disposizioni contenute nella presente Policy:
Integrare i seguenti documenti::

- Regolamento di Istituto (sanzioni relative all'utilizzo scorretto e al danneggiamento dei dispositivi forniti dalla scuola .
- Patto di corresponsabilità,(genitori)
- Curriculum verticale (adeguamento competenze digitali)

Installare la scatola/box per le segnalazioni degli studenti in ogni plesso.
Nominare i referenti per le segnalazioni.

Per la commissione Generazioni Connesse
la referente del progetto

Prof.ssa M. Raffaella Ratti

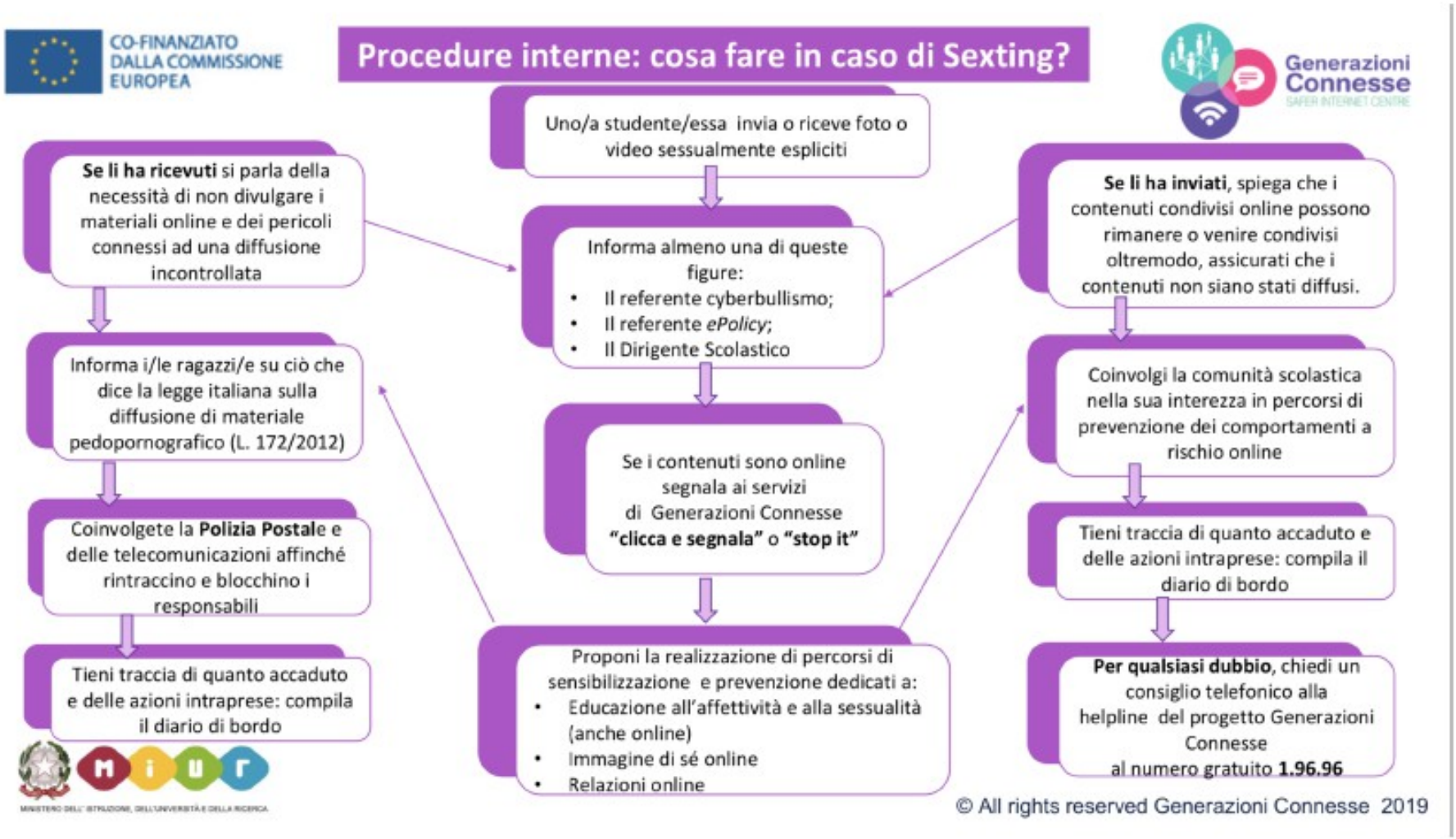
La dirigente

Prof.ssa Anna Maria Florio

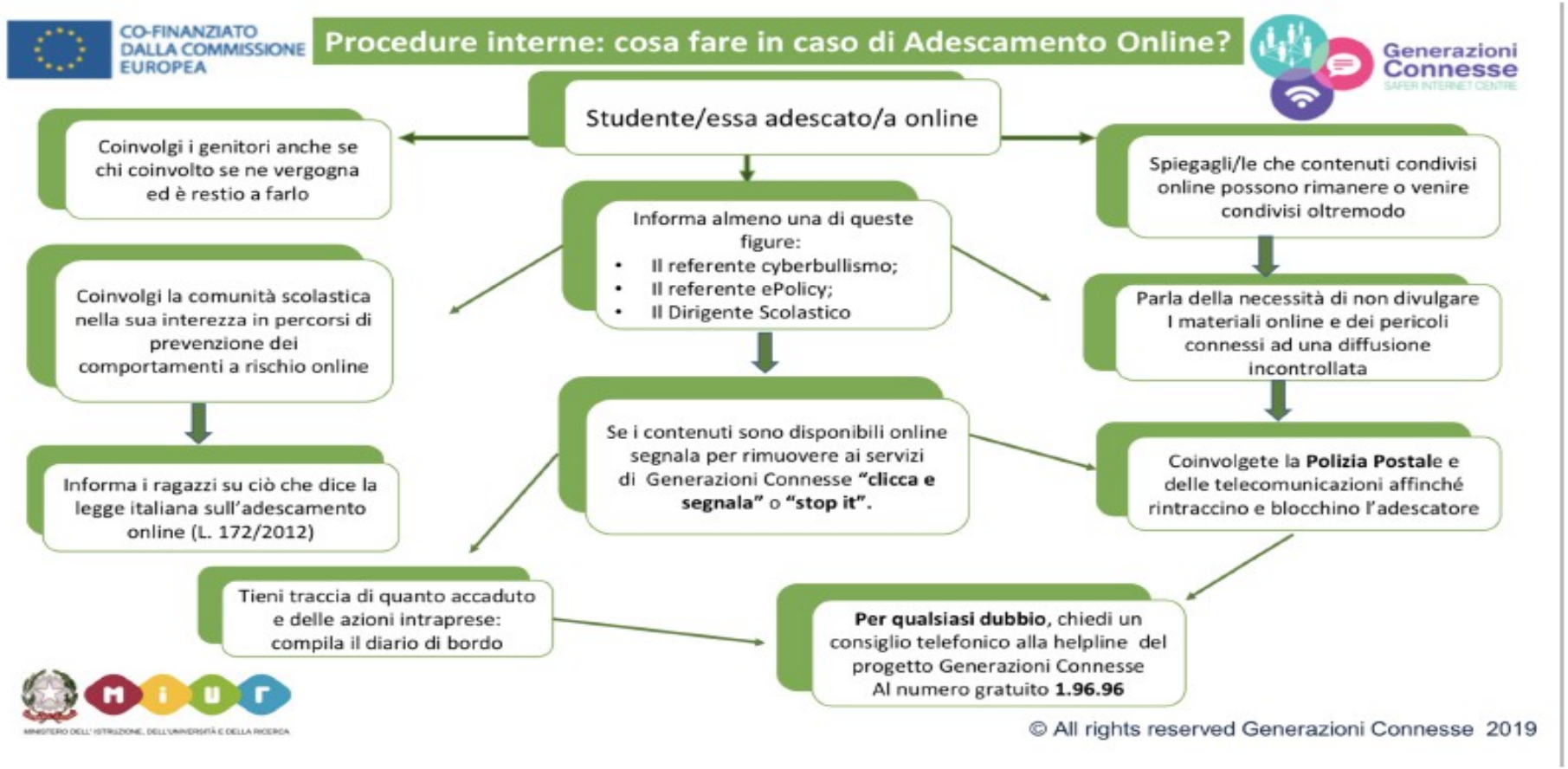
Si allegano i seguenti documenti proposti dalla piattaforma di “Generazioni Connesse” per le procedure di intervento sui casi e per la loro segnalazione..

Procedura di intervento in caso di sexting
Procedura di intervento in caso di adescamento
Procedura di intervento per esterni.
Schede di segnalazione
Diario di bordo

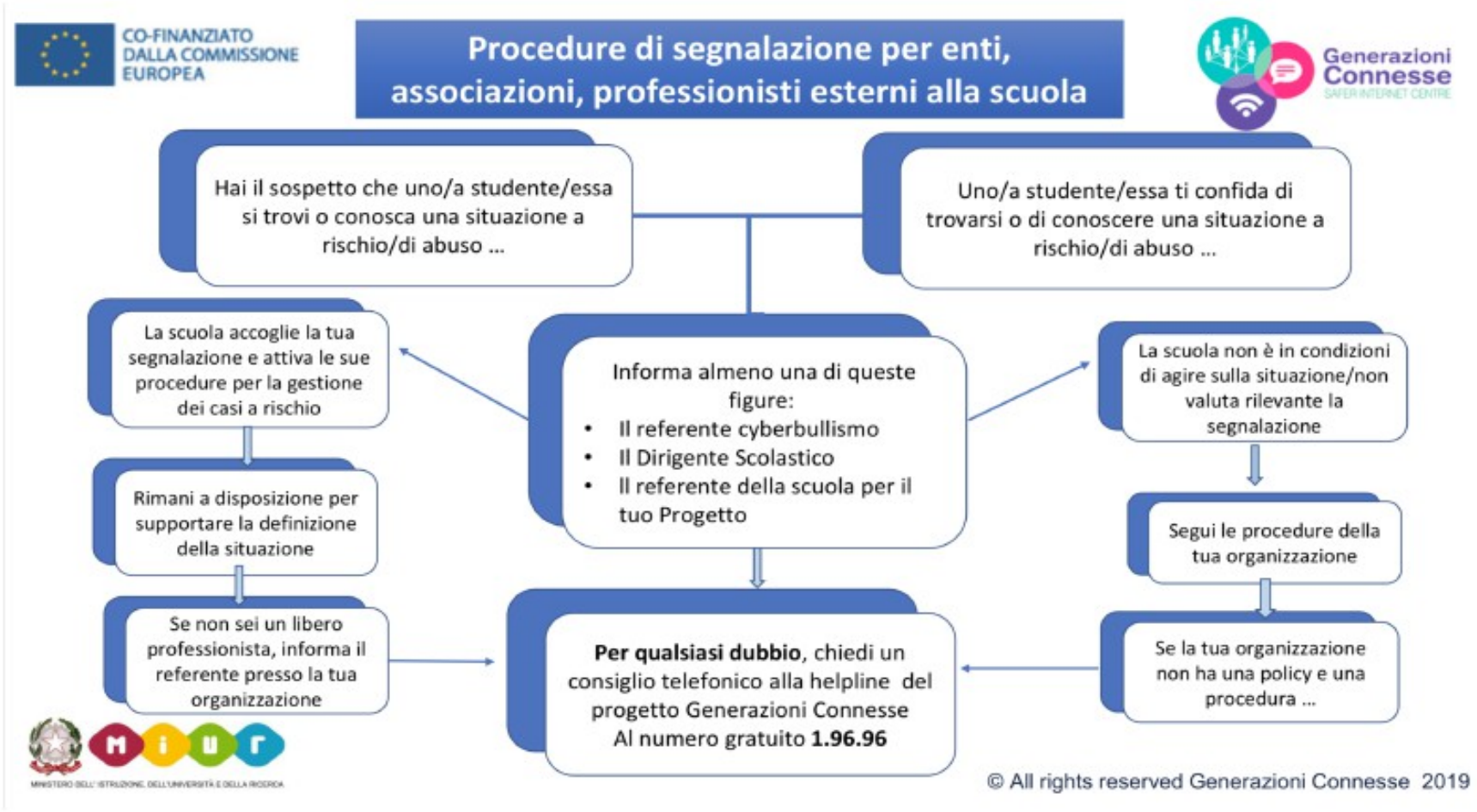
Procedura di intervento in caso di sexting



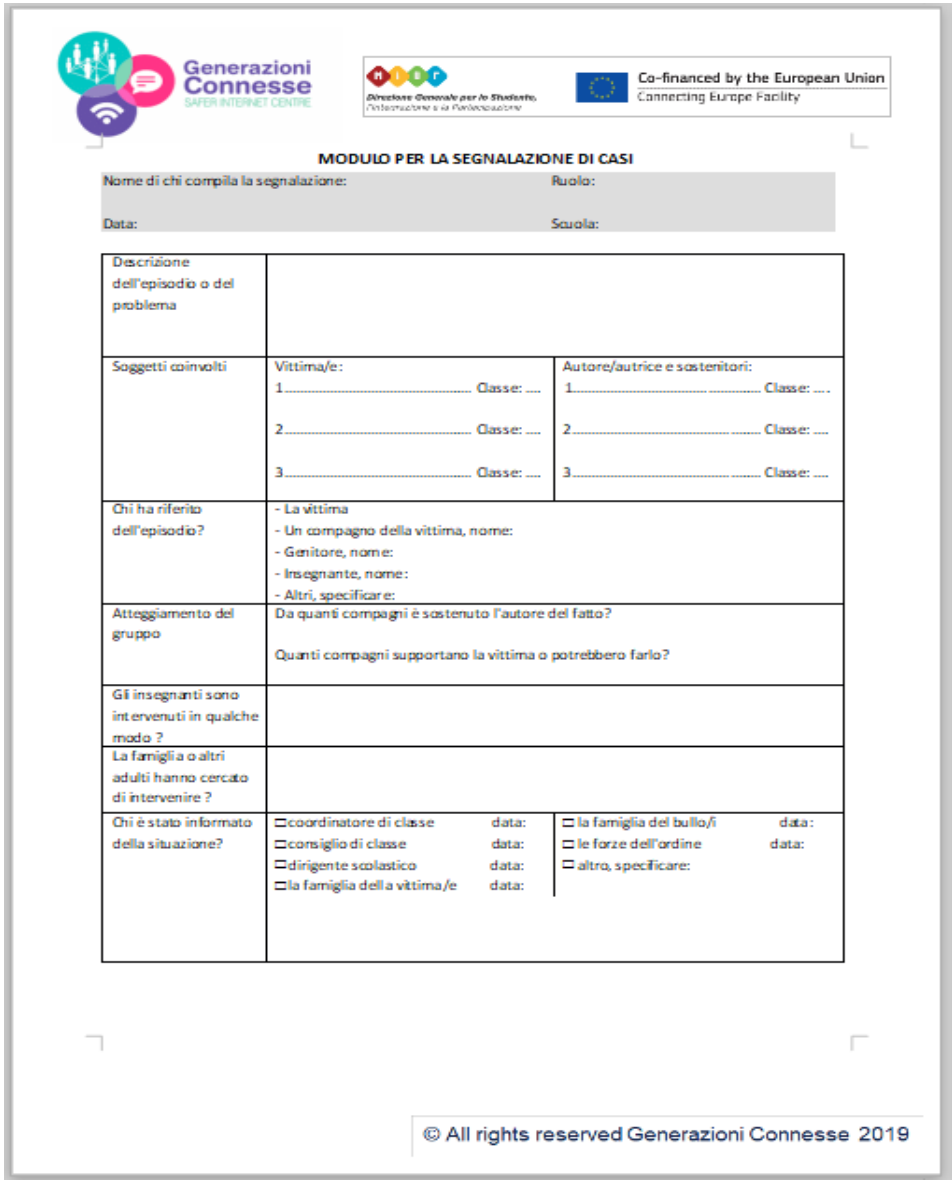
Procedura di intervento in caso di adescamento



Procedura di intervento per esterni alla scuola



Schede di segnalazione



Generazioni Connesse
SAFER INTERNET CENTRE

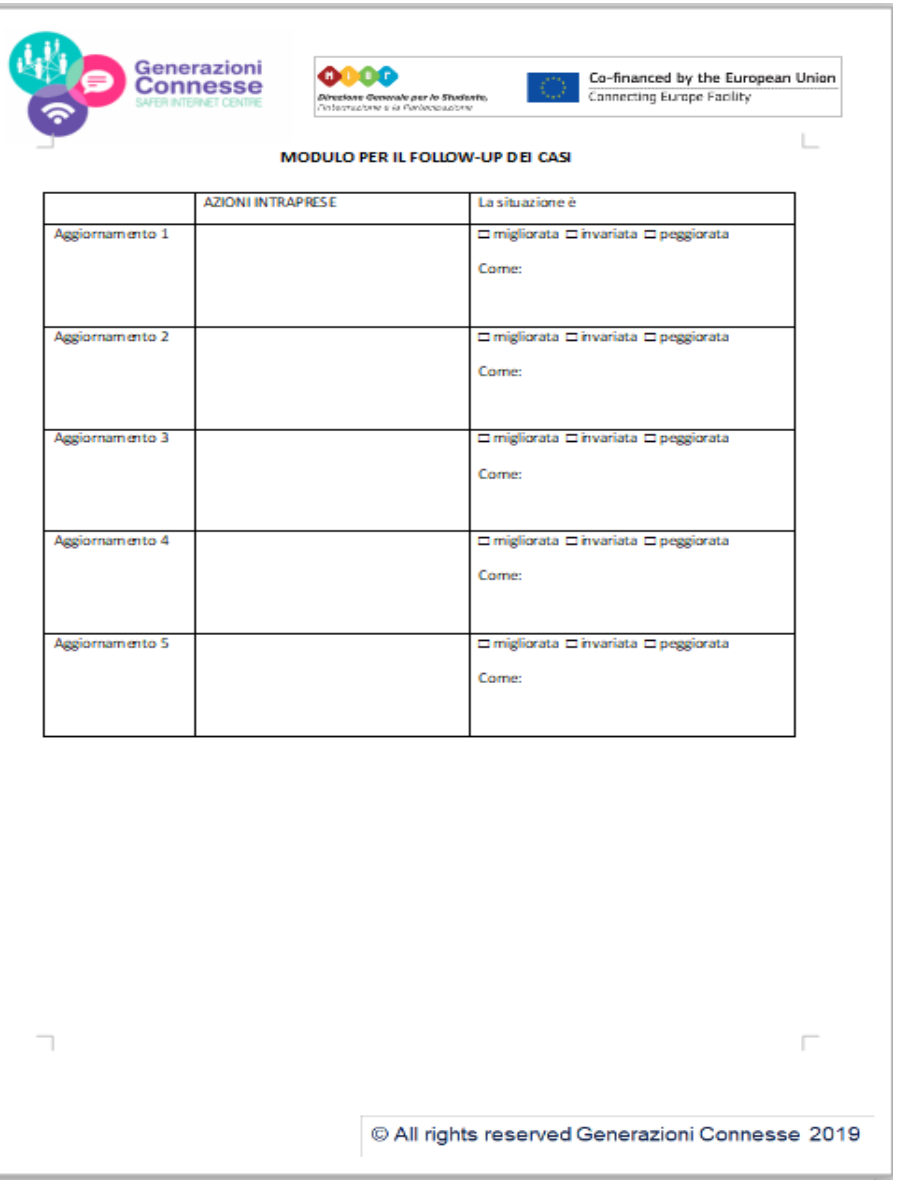
Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Co-financed by the European Union
Connecting Europe Facility

MODULO PER LA SEGNALAZIONE DI CASI

Nome di chi compila la segnalazione:	Ruolo:
Data:	Scuola:

Descrizione dell'episodio o del problema		
Soggetti coinvolti	Vittima/e: 1..... Classe: .... 2..... Classe: .... 3..... Classe:	Autore/autrice e sostenitori: 1..... Classe: .... 2..... Classe: .... 3..... Classe: ....
Chi ha riferito dell'episodio?	- La vittima - Un compagno della vittima, nome: - Genitore, nome: - Insegnante, nome: - Altri, specificare:	
Atteggiamento del gruppo	Da quanti compagni è sostenuto l'autore del fatto? Quanti compagni supportano la vittima o potrebbero farlo?	
Gli insegnanti sono intervenuti in qualche modo ?		
La famiglia o altri adulti hanno cercato di intervenire ?		
Chi è stato informato della situazione?	☐coordinatore di classe data: ☐consiglio di classe data: ☐dirigente scolastico data: ☐la famiglia della vittima/e data:	☐ la famiglia del bullo/i data: ☐ le forze dell'ordine data: ☐ altro, specificare:



Generazioni Connesse
SAFER INTERNET CENTRE

Direzione Generale per lo Studente, l'Integrazione e la Partecipazione

Co-financed by the European Union
Connecting Europe Facility

MODULO PER IL FOLLOW-UP DEI CASI

	AZIONI INTRAPRESE	La situazione è
Aggiornamento 1		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 2		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 3		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 4		☐ migliorata ☐ invariata ☐ peggiorata Come:
Aggiornamento 5		☐ migliorata ☐ invariata ☐ peggiorata Come:

Diario di bordo

CO-FINANZIATO DALLA COMMISSIONE EUROPEA

Sicurezza in rete - Schema per la scuola

Generazioni Connesse

Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi
Scuola _____ Anno Scolastico _____

N°	Data	ora	Episodio *(riassunto)*	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		