ISTITUTO COMPRENSIVO DI SCUOLA INFANZIA PRIMARIA SECONDARIA 1°GR.
"L. ARIOSTO" VIA SASSO, 3 42032 BUSANA (RE)
c.f. 80016110357 tel. 0522/891150 WWW.ICBUSANA.EDU.IT
e-mail: segreteria@icbusana.edu.it pec: reic81600g@pec.istruzione.it

E - safety policy

a.s. 2021 – 2022

1. INTRODUZIONE

La scuola elabora il presente documento seguendo le indicazioni delle Linee di Orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo (aprile 2015) elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con "Generazioni Connesse" e il Safer Internet Center per l'Italia. Si recepiscono, altresì, le integrazioni e le modifiche necessarie in linea con i recenti interventi normativi con particolare riferimento alle innovazioni introdotte con l'emanazione della L. 71/2017 "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" e DM 18/2021 “Linee di orientamento per la prevenzione e il contrasto dei fenomeni di bullismo e cyberbullismo”.
Tale documento è da intendersi quale strumento flessibile e suscettibile di periodici aggiornamenti tale da rispondere alle sfide educative e pedagogiche derivanti dall'evolversi costante e veloce delle nuove tecnologie.

1.1 Scopo della policy

Nel corso degli ultimi anni, il nostro Istituto Comprensivo ha svolto una crescente azione mirata ad incrementare l’uso delle tecnologie informatiche nella didattica e nell’organizzazione generale della scuola, in conformità con il Piano Nazionale Scuola Digitale. Da ciò è nata l’esigenza di redigere un documento di E-Safety Policy.

L’intento è dare al nostro Istituto un impulso allo sviluppo di una cultura d’uso corretto e consapevole di Internet, mediante il richiamo a norme vigenti e tramite l’indicazione di procedure opportune per un uso sempre più professionale da parte dell’intera comunità scolastica.

Lo scopo della E-Safety Policy è:

- ✓ stabilire i principi fondamentali tipici di tutti i membri della comunità scolastica per quanto riguarda l'utilizzo di tecnologie;
- ✓ salvaguardare e proteggere i bambini, i ragazzi e lo staff dell'Istituto;
- ✓ assistere il personale della scuola a lavorare in modo sicuro e responsabile con altre tecnologie di comunicazione di Internet e monitorare i propri standard e le prassi;
- ✓ impostare chiare aspettative di comportamento e/o codici di condotta rilevanti per un uso responsabile di Internet a scopo didattico, personale o ricreativo;
- ✓ affrontare gli abusi online come il cyberbullismo, che sono riferimenti incrociati con le altre politiche della scuola;
- ✓ garantire che tutti i membri della comunità scolastica siano consapevoli del fatto che il comportamento illecito o pericoloso è inaccettabile e che saranno intraprese le opportune azioni disciplinari e giudiziarie.

Nello specifico, la nostra Policy di e-Safety avrà lo scopo di delineare:

1. **misure atte a facilitare e promuovere** l'utilizzo delle TIC nella didattica, cioè azioni utili a

sviluppare le competenze digitali, che costituiscono anche misure di prevenzione, come si vedrà più avanti;

2. **misure di prevenzione**, ossia azioni finalizzate alla prevenzione nella scuola di fenomeni legati ai rischi delle tecnologie digitali;
3. **misure per la segnalazione e gestione dei casi**, ovvero disposizioni semplici su come segnalare i casi nella scuola, comprese informazioni su chi sono le figure di riferimento, sugli strumenti a disposizione, sull'iter successivo alla segnalazione e su quali misure di tutela può contare chi segnala e su come gestire eventuali casi che si andranno a verificare.

Il regolamento va inteso non come un semplice divieto nato da generici timori, ma come stimolo ad un uso consapevole e critico delle tecnologie informatiche, con la dovuta competenza a seconda dei diversi gradi di utilizzo.

1.2 Ruoli e responsabilità

Il personale dell'Istituto, i genitori e gli alunni, si impegnano formalmente nel rispettare quanto riportato nel documento, in un'ottica di consapevolezza e legalità, poiché non va dimenticato che la fruizione di Internet è tutelata e sanzionata da Leggi dello Stato.

Ferme restando le strategie sistematiche messe in atto dalla Scuola ciascun utente connesso alla rete deve:

- ✓ rispettare il presente regolamento e la legislazione vigente;
- ✓ tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso;
- ✓ rispettare la cosiddetta netiquette (regole condivise che disciplinano il rapportarsi fra utenti della rete, siti, forum, mail e di qualsiasi altro tipo di comunicazione) cui si rimanda ai successivi paragrafi.

Di seguito vengono indicati i ruoli e gli incarichi dei diversi soggetti coinvolti.

Dirigente scolastico

E' responsabile e garantisce la sicurezza di tutti i membri della comunità scolastica deve pertanto:

- ✓ garantire la sicurezza (tra cui la sicurezza on-line) dei membri della comunità scolastica;
- ✓ garantire la corretta formazione del personale scolastico relativo all'uso delle TIC nella didattica e sulle tematiche relative all'uso sicuro e consapevole di Internet e della rete;
- ✓ garantire l'esistenza di un sistema in grado di consentire il monitoraggio e il controllo interno della sicurezza on-line;
- ✓ monitorare che le azioni svolte dai docenti siano conformi al regolamento;

- ✓ intervenire in caso di violazione del regolamento da parte dei docenti o degli alunni, attivando tutto quanto previsto dal Regolamento d'Istituto al capitolo inerente le sanzioni disciplinari da comminare a quanti, studenti o personale scolastico dovessero contravvenire a quanto previsto dal regolamento stesso.

Animatore digitale

Il suo profilo professionale è rivolto a:

- ✓ formazione interna, per stimolare la formazione del personale e delle scolaresche negli ambiti del Piano Nazionale Scuola Digitale (PNSD), anche in tema di uso consapevole e corretto delle potenzialità offerte dalla rete, favorendo la partecipazione di tutta la comunità scolastica a tali attività formative;
- ✓ coinvolgimento della comunità scolastica, per favorire la conoscenza e la condivisione degli studenti, delle famiglie e di altre figure del territorio sui temi del PNSD afferenti al "Safer internet";
- ✓ creazione di soluzioni innovative, per individuare soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno dell'Istituzione scolastica, coerenti con l'analisi dei fabbisogni dell'Istituto stesso, in un'ottica trasversale di sicurezza di rete.

Referente e team emergenza Bullismo - cyberbullismo

Il docente referente, coadiuvato dai membri del TEAM EMERGENZA, svolge un importante compito di supporto al dirigente scolastico su diversi aspetti inerenti rispettivamente:

- ✓ alla revisione/stesura dei Regolamenti (e-Safety, Regolamento d'istituto, patto di corresponsabilità), atti e documenti (PTOF, PdM, Rav).
- ✓ alle iniziative e azioni di prevenzione e contrasto del Cyberbullismo; avvalendosi, a tal fine, della collaborazione delle Forze di polizia e delle associazioni e dei centri attivi sul territorio;
- ✓ alla promozione della formazione di alunni, famiglie e personale
- ✓ alla consulenza;
- ✓ alla promozione di attività o progetti da svolgere nelle classi;
- ✓ all'applicazione e al controllo dei protocolli di rilevazione, monitoraggio e gestione delle potenziali azioni di cyberbullismo;
- ✓ alla diffusione della E- Safety Policy in tutte le forme che si riterranno necessarie (power point, incontri on line, schede semplificative..).

Insegnanti

I docenti sono invitati ad utilizzare nella propria didattica ed attività educativa tutti gli strumenti offerti dalle nuove tecnologie che ritengono più efficaci ed idonei, nel libero esercizio della propria professionalità, in coerenza con le linee del progetto educativo e del PTOF d'Istituto.
I docenti sono inoltre chiamati a sorvegliare attentamente sugli alunni loro affidati affinchè

rispettino le regole e le indicazioni, nonché mantengano in buono stato ed utilizzino in modo adeguato ed opportuno tutti i mezzi tecnologici a disposizione. I docenti devono:

- ✓ avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- ✓ aver preso visione della presente policy;
- ✓ segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'Animatore digitale per le opportune indagini/azioni/sanzioni;
- ✓ mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici;
- ✓ integrare i problemi di sicurezza informatica in tutti gli aspetti del curricolo di studi e in altre attività extracurricolari;
- ✓ far comprendere e mettere in pratica alla componente studentesca le regole di comportamento relative alla sicurezza informatica;
- ✓ controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche ecc. nelle lezioni e nelle altre attività scolastiche che ne prevedono la necessità a scopi didattici;
- ✓ guidare la navigazione di studentesse e studenti, nelle lezioni in cui l'uso di Internet è pianificato, verso siti controllati come idonei per il loro uso, onde evitare di incontrare materiali inadatti;
- ✓ non fare uso di dispositivi di carattere personale (telefoni cellulari, tablet..) se non per esclusivo uso didattico;
- ✓ non salvare sui propri dispositivi personali alcun dato lesivo della privacy.

L'insegnante può predisporre attività didattiche in grado non solo di migliorare l'apprendimento in termini di conoscenze e di competenze, ma anche indirizzate a far acquisire agli studenti una "conoscenza critica" e una consapevolezza del proprio "agire tecnologico".

A tal fine può essere utile:

- ✓ illustrare ai propri allievi le regole di utilizzo delle nuove tecnologie contenute nel presente documento;
- ✓ discutere con i propri allievi delle regole della *E-safety policy*;
- ✓ vigilare affinché gli allievi utilizzino Internet solamente sotto la sua supervisione;
- ✓ dare chiare indicazioni agli alunni su come si utilizzano Internet, la posta elettronica e gli altri sistemi di messaggistica istantanea;
- ✓ monitorare la navigazione affinché gli alunni non accedano a siti non autorizzati;
- ✓ cercare e consigliare siti appropriati per le ricerche degli allievi.

Studenti

Tutti gli alunni sono responsabili per l'utilizzo corretto dei sistemi informatici e della tecnologia digitale in accordo con i termini previsti da questa policy. Ogni comportamento che, pur nel rispetto

delle singole norme, sia volto a perseguire finalità diverse da quelle pedagogiche, educative e didattiche, non è consentito.

In particolare sono tenuti a:

- ✓ utilizzare le ICT loro assegnate dai docenti e/o dalla scuola per lo svolgimento delle attività autorizzate, sotto la supervisione del docente;
- ✓ non utilizzare dispositivi personali durante le attività didattiche se non espressamente consentito dal personale docente;
- ✓ archiviare i propri documenti secondo le modalità indicate dai docenti e chiudere sempre correttamente la propria sessione di lavoro al termine del suo utilizzo;
- ✓ non eseguire tentativi di modifica della configurazione del sistema delle macchine;
- ✓ non utilizzare giochi né in locale né in rete;
- ✓ non installare sulle macchine di uso comune (laboratori, PC di classe, etc.) software e ogni altra applicazione non espressamente autorizzata dal docente responsabile;
- ✓ comunicare tempestivamente ai docenti responsabili il riscontro di eventuali malfunzionamenti della strumentazione e/o di comportamenti scorretti, pericolosi o inappropriati da parte propria o di altri;
- ✓ mantenere segrete e custodire con cura eventuali password;
- ✓ avere una buona comprensione delle possibilità di ricerca sul web e della necessità di evitare il plagio, rispettare le normative sul diritto d'autore, non diffondere dati personali;
- ✓ comprendere l'importanza della segnalazione di ogni abuso, uso improprio o accesso a materiali inappropriati e conoscere il protocollo per tali segnalazioni;
- ✓ conoscere e comprendere le politiche sull'uso di dispositivi mobili e di macchine fotografiche digitali;
- ✓ capire le politiche di utilizzo delle immagini ed essere consapevoli del significato e della gravità del cyberbullismo;
- ✓ capire l'importanza di adottare buone pratiche di sicurezza informatica in tutti i momenti della vita, a tutela dell'incolumità propria e altrui e per evitare di perpetrare reati punibili sia a livello scolastico sia da parte della magistratura;
- ✓ discutere sempre e confrontarsi apertamente con i propri docenti in caso di dubbi o di incertezze sui comportamenti più appropriati da adottare in relazione alle ICT dell'Istituto;
- ✓ non utilizzare a scuola telefoni cellulari e altri dispositivi elettronici (macchine digitali, smartphones, I-Pod, Playstation, registratori audio, tablet, etc.) se non per svolgere l'attività didattica: i genitori sono responsabili per qualsiasi utilizzo non consentito, in particolare se si tratta di diffusione di foto/video/audio non autorizzati dagli interessati e/o lesivi della dignità o della reputazione dei soggetti ripresi, così come stabilito dal Regolamento d'Istituto.

Famiglie

Le famiglie degli alunni sono invitate a collaborare con la scuola per una efficace educazione dei ragazzi ad un utilizzo corretto e sicuro delle TIC, in un rapporto di costruttivo "dialogo educativo".

Ai genitori (o esercenti la patria potestà) viene richiesto:

- ✓ di prestare attenzione ai principi e alle regole per un corretto utilizzo delle ICT, sintetizzate in questo documento, nonché di segnalare e confrontarsi prontamente con docenti e coordinatori di classe, qualora abbiano il sospetto ovvero fondata conoscenza di comportamenti pericolosi o inappropriati da parte dei propri figli relativamente alle TIC della scuola;
- ✓ di leggere e firmare la Dichiarazione liberatoria per la pubblicazione di elaborati, nomi, voci, immagini, materiale audiovisivo sul sito della scuola e attraverso altri canali di comunicazione.

Allo scopo di condividere regole comuni per l'utilizzo sicuro di Internet sia a casa che a scuola, per il bene dei bambini e ragazzi, si invitano i genitori o chi ne fa le veci a prestare la massima attenzione ai principi e alle regole per un utilizzo consapevole delle TIC, sintetizzate in questo documento, impegnandosi a farle rispettare ai propri figli, possibilmente anche in ambito domestico.

I genitori saranno incoraggiati a sostenere la scuola nel promuovere le buone pratiche di e-safety e a seguire le linee guida sull'uso appropriato di:

- ✓ immagini digitali e video registrati in occasione di eventi scolastici, anche al di fuori delle aule;
- ✓ accesso alle sezioni del sito dedicate ai genitori, con particolare riguardo al registro elettronico;
- ✓ dispositivi personali dei loro figli nella scuola.

In ogni caso, una positiva, costruttiva e collaborativa relazione educativa in dialogo tra scuola e famiglia è la migliore forma di tutela e di prevenzione relativa ad ogni forma di comportamento illecito o potenzialmente pericoloso per alunni, famiglie e Istituto.

1.3 Condivisione e comunicazione della Policy all'intera comunità scolastica

Questa policy si applica a tutti i membri della comunità scolastica che hanno accesso o che sono utenti dei sistemi informatici della scuola. In particolare essa viene redatta per regolare il comportamento della componente studentesca dentro le aule scolastiche e per sensibilizzarli all'adozione di buone pratiche quando sono fuori dalla scuola e autorizza i membri del personale docente a erogare sanzioni disciplinari per comportamenti inappropriati avvenuti all'interno dell'istituzione scolastica.

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

- ✓ condivisione in sede di organi collegiali preposti e inserimento nel PTOF;
- ✓ pubblicazione della E-Safety Policy sul sito della scuola;
- ✓ comunicazione a genitori e alunni all'inizio dell'anno scolastico e nelle attività di orientamento;

- ✓ fornire informazioni agli studenti sull'uso responsabile della rete in modo tale che possano sviluppare "comportamenti sicuri";
- ✓ fornire informazioni al personale, agli alunni ed ai genitori su come segnalare azioni di bullismo o cyber-bullismo.

1.4 Integrazione della Policy con Regolamenti esistenti

Il documento è allegato al Regolamento di Istituto e parte integrante dello stesso; viene assunto a delibera dal Collegio Docenti e ratificato dal Consiglio d'Istituto; è pubblicato sul sito WEB della scuola e potrà essere revisionato annualmente.

Con questo atto si vuole attivare e mantenere nella nostra scuola una Policy di E-safety in materia di ''Tecnologie dell'Informazione e della Comunicazione" (TIC) da tutti accettata.

1.5 Monitoraggio dell'implementazione della Policy e suo aggiornamento

Questo documento verrà revisionato annualmente e, se necessario, verranno messe in atto tutte le azioni migliorative che il Collegio dei Docenti riterrà opportuno attuare al fine di rendere la Policy di E-safety sempre più parte viva ed integrante del Regolamento e del PTOF d'Istituto.

1.6 Gestione delle infrazioni alla Policy

Le infrazioni alla policy possono essere rilevate da docenti/ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti/ATA/DS.

In particolare si attueranno le seguenti operazioni:

- ✓ Osservare in modo attento e partecipe quanto accade;
- ✓ Confrontarsi con il Dirigente scolastico e valutare l'opportunità di informare la famiglia per creare una rete di supporto e un piano d'azione condiviso;
- ✓ Coinvolgere se possibile nel dialogo e confrontarsi con animatore digitale e referente bullismo - cyberbullismo della scuola;
- ✓ Attivare le forze dell'ordine competenti o i servizi del territorio più adeguati, qualora la situazione specifica lo richieda.

Qualora esse si configurino come vero e proprio reato, occorre darne tempestiva segnalazione al Dirigente Scolastico per gli adempimenti del caso.
La violazione o il dolo accertati, oltre all'intervento disciplinare, daranno luogo alla richiesta di risarcimento nella misura del danno provocato e comunque decisa dal Dirigente Scolastico. Rimangono, inoltre, applicabili ulteriori sanzioni disciplinari e azioni civili per danni, nonché l'eventuale denuncia all'autorità giudiziaria qualora la violazione si configuri come reato.

Al personale e agli alunni saranno date informazioni sulle infrazioni in uso e le eventuali sanzioni contenute nel Regolamento di Istituto o nel presente documento. Nel caso in cui le infrazioni della policy violino norme previste dal Regolamento di Istituto si procede secondo quanto previsto dal Regolamento stesso; qualora le infrazioni riguardino l'opportunità di certi comportamenti o la convivenza civile, la scuola eroga delle sanzioni secondo il principio della sensibilizzazione e del risarcimento dell'eventuale danno provocato, in uno spirito di recupero e rieducazione.

Il Dirigente scolastico ha la facoltà di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (pc, tablet, notebook, ecc) a chi non si attiene alle regole stabilite.

In caso di violazioni delle norme stabilite dal presente documento e/o di danneggiamenti alle macchine la scuola adotterà sanzioni disciplinari rapportate alla gravità degli episodi.

Qualsiasi rilevamento di sospetto abuso, offesa, procurato disagio ricevuto su internet, sarà sempre riferito al Dirigente Scolastico e all'animatore digitale e/o referente del bullismo, che fungeranno da primo punto di contatto. Gli interventi saranno quindi commisurati al tipo di infrazione e al soggetto coinvolto nella stessa.

Infrazioni degli alunni

Le potenziali infrazioni in cui è possibile che gli alunni incorrano a scuola nell'utilizzo delle tecnologie digitali di internet di cui si dispone per la didattica, in relazione alla fascia di età considerate, sono prevedibilmente le seguenti:

- ✓ un uso della rete e delle App ad essa collegate per offendere, giudicare, infastidire o impedire, in modo persistente, a qualcuno di esprimersi o partecipare;
- ✓ l'invio incauto o senza permesso di foto o di altri dati personali;
- ✓ l'invio o la condivisione di immagini intime o troppo spinte;
- ✓ il collegamento a siti web, nell'orario scolastico, non autorizzati dai docenti.
- ✓ l'utilizzo, non autorizzato o comunicato ai docenti, dello smartphone in orario scolastico (utilizzando messaggeria, video , audio o foto).

Gli interventi correttivi previsti per gli alunni sono rapportati all'età e al livello di sviluppo, al tipo di comportamento messo in atto; le possibili azioni di intervento possono prevedere:

- ✓ ritiro del cellulare fino a fine giornata;
- ✓ informazione e confronto con i genitori/tutori per condividere le strategie più opportune;
- ✓ provvedimenti disciplinari, commisurati all'età e all'entità del fatto, quali:
  - il richiamo verbale;
  - il richiamo scritto con annotazione sul diario;
  - la nota disciplinare sul registro (erogata dal consiglio di classe);
  - la convocazione dei genitori da parte degli insegnanti o del DS.

I genitori sono invitati a supportare la scuola per mettere a punto azioni di contrasto efficaci.
Denunce di bullismo online saranno trattate in conformità con la legge attuale.

Reclami relativi alla protezione dei dati saranno trattati in conformità alle procedure di protezione dei Dati regolamentate dal Regolamento Privacy vigente.

Infrazioni del personale

Le potenziali infrazioni in cui è possibile che il personale scolastico, in particolare i docenti, incorrano nell'utilizzo delle tecnologie digitali e di internet sono diverse e alcune possono determinare, favorire o avere conseguenze di maggiore o minore rilievo sull'uso corretto e responsabile delle TIC anche da parte degli alunni:

- ✓ un utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di insegnamento o al profilo professionale, anche tramite installazione di software o il salvataggio di materiali non idonei;
- ✓ un utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- ✓ un trattamento dei dati personali, comuni e sensibili degli alunni, non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- ✓ una diffusione delle password assegnate e una custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- ✓ una vigilanza elusa sugli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili incidenti;
- ✓ insufficienti interventi nelle situazioni critiche di contrasto a terzi, correttivi o di sostegno agli alunni, di segnalazione ai genitori, al Dirigente scolastico, all'Animatore digitale.

Il Dirigente scolastico interverrà dando avvio a procedimenti che possono avere carattere organizzativo, gestionale, disciplinare, amministrativo, penale a seconda del tipo o della gravità delle infrazioni commesse.
Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

Ruolo dei genitori

In considerazione dell'età degli alunni e della loro dipendenza dagli adulti, anche alcune condizioni e condotte dei genitori possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli alunni a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.
Le situazioni familiari meno favorevoli sono:

- ✓ una piena autonomia concessa al proprio figlio nella navigazione sul web e nell'utilizzo dei device senza una periodica condivisione o controllo dei contenuti;
- ✓ la mancanza di adeguata conoscenza che la responsabilità dei contenuti veicolati dai minori è sempre ascrivibile ai genitori/tutori ;
- ✓ assoluto disinteresse sui contenuti dello smartphone dei propri figli.

I genitori degli alunni possono essere convocati a scuola per concordare misure educative diverse oppure essere sanzionabili a norma di legge in base alla gravità dei comportamenti dei loro figli, se dovessero risultare pericolosi per sé e/o dannosi per gli altri.

2. FORMAZIONE E CURRICOLO

L'Istituto persegue relativamente al Curricolo digitale le indicazioni contenute nel PNSD, nelle Raccomandazioni del Parlamento Europeo relative alle competenze chiave e nelle Indicazioni Nazionali per il Curricolo del 2012.
In sintesi:

"La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa è supportata da abilità di base nelle TIC: l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet" (Raccomandazione del Parlamento Europeo relativa alle competenze chiave per l'apprendimento permanente).

2.1 Curricolo sulle competenze digitali per gli studenti

L'uso delle TIC è inserito pertanto nel curricolo d'Istituto e integrato nel Curricolo di Educazione Civica; le competenze specifiche sono enucleate nella sezione "Competenze digitali" inserito nel Curricolo d'Istituto delle competenze chiave europee.

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

Negli ultimi anni la Comunità Europea ha individuato con chiarezza alcuni importanti obiettivi strategici legati al ruolo delle tecnologie dell'informazione e della comunicazione nell'esperienza quotidiana delle nuove generazioni. L'Italia ha rapidamente recepito e condiviso le linee guida dettate dalla UE in materia di nuove tecnologie, in particolare nell'ambito dell'istruzione.

In quest'ottica il nostro Istituto ha tra i docenti molti insegnanti che hanno aderito ad iniziative atte a raggiungere un buon livello di formazione in merito all'utilizzo e l'integrazione delle TIC nella didattica, non dimenticando mai l'importanza dell'autoformazione continua per rimanere sempre aggiornati in merito ad un mondo in continua evoluzione.

Nel PTOF si prevede che una parte della formazione in servizio obbligatoria ai sensi della L. 107/2015 sia dedicata proprio all'uso e all'inserimento delle TIC nella didattica e ai temi informatici in generale.

Inoltre ci si è mossi promuovendo diverse azioni rivolte al personale:

- ✓ la somministrazione di un questionario rivolto al personale per la rilevazione dei bisogni "digitali";
- ✓ la formazione dei docenti all'utilizzo delle App di Google Workspace for Education, registro elettronico e lo scrutinio elettronico;
- ✓ la ricognizione e messa a punto delle dotazioni digitali;
- ✓ l'attivazione e comunicazione di iniziative di formazione, in particolare rivolte allo sviluppo e alla diffusione del Coding e del pensiero computazionale;
- ✓ la formazione del personale in materia di sicurezza on-line attraverso corsi di formazione e/o aggiornamento;
- ✓ il monitoraggio del piano digitale di Istituto e dei risultati conseguiti.

2.3 Sensibilizzazione delle famiglie

L'istituzione scolastica deve offrire contenuti online sicuri, affidabili, di facile comprensione per migliorare l'insegnamento/apprendimento e gli utenti devono affrontare in modo consapevole i pericoli della rete per riqualificare la propria vita privata, professionale e relazionale.

Si prevede l'attuazione di un programma continuativo di informazione, consulenza e orientamento per i genitori, attraverso:

- ✓ la presentazione ai genitori del regolamento della Policy, al fine di garantire che i principi di comportamento sicuro on-line siano chiari;
- ✓ la protezione da contenuti inadeguati e illegali dei bambini e degli adolescenti;
- ✓ l'educazione ad un utilizzo consapevole, nel rispetto delle leggi in materia;
- ✓ la sicurezza dei sistemi informatici;
- ✓ la sicurezza in ingresso e in uscita delle informazioni condivise mediante l'uso delle TIC;
- ✓ la protezione dei dati personali;
- ✓ informazioni sui siti nazionali di sostegno per genitori, quali il sito www.generazioniconnesse.it.

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

La scuola si prefigge di mettere in atto tutte le azioni necessarie per garantire agli studenti l'accesso alla documentazione cercata adottando tutti i sistemi di sicurezza conosciuti per diminuire e limitare il più possibile le possibilità di rischio durante la navigazione.

3.1 Accesso ad Internet: filtri sulla navigazione e antivirus

Il diritto di accesso a Internet è 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 infatti 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”.

Nel nostro Istituto tale diritto è garantito in diverse forme:

- ✓ Presso la sede centrale (Scuola secondaria di primo grado di Busana) è attivo una protezione firewall, la navigazione avviene attraverso una rete dedicata (HOTSPOT ARIOSTO) cui si accede tramite voucher personale che permette il monitoraggio del traffico web ed il blocco dell'accesso a siti inappropriati ad un contesto scolastico.
- ✓ Nelle restanti sedi il diritto di accesso è comunque garantito dalla connessione di rete protetta da password, monitorata dal personale in servizio sui plessi.
- ✓ Si prevede di ampliare la protezione firewall nelle altre sedi dell’Istituto.
- ✓ Occorre, inoltre, sensibilizzare tutta la comunità scolastica sull'opportunità di mantenere aggiornati gli antivirus installati sulle macchine personali mentre i dispositivi dell’Istituto risultano tutti protetti da antivirus di sistema di cui si controlla periodicamente l’aggiornamento.

3.2 Nomina dell’amministratore di sistema

L’Istituto ha conferito alla ditta “Bagnoli Net” il ruolo di Amministratore di sistema nella sede centrale; tra i compiti assegnati si sottolinea:

- ✓ configurazione dei servizi di accesso a internet tramite la rete interna
- ✓ attivazione della password di accensione (BIOS);
- ✓ creazione di un’area condivisa sul server per lo scambio di dati tra i vari utenti, evitando condivisioni dei dischi o di altri supporti configurati nel PC che non siano strettamente necessarie poiché possono essere un canale per i software che minacciano la sicurezza dell’intero sistema;
- ✓ distruzione delle unità di memoria interne alla macchina (hard - disk, memorie allo stato solido) ogni qualvolta si procederà alla dismissione (procedura discarico inventariale) di un PC e dei supporti removibili consegnati a tale scopo dagli utenti;
- ✓ utilizzo delle credenziali di amministrazione del sistema per accedere ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un utente in caso di indispensabile ed indifferibile necessità di intervento per prolungata assenza, irrintracciabilità o impedimento dello stesso, solo per il tempo necessario al compimento di attività indifferibili e solo su richiesta del Responsabile del trattamento.

L’Amministratore di sistema, nell’espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, e dopo aver richiesto l’autorizzazione all’utente interessato, al PC di ciascun utente.

3.3 Gestione accessi (rete e registro elettronico)

Gli accessi alle TIC sono gestiti sotto diverse forme:

- ✓ Il personale accede alla rete della scuola con una password protetta che nel caso della sede centrale corrisponde ad un voucher nominale.
- ✓ I docenti accedono al registro elettronico tramite password personale valevole per il periodo di servizio presso l'Istituto la cui sicurezza è garantita dalla periodica modifica di "cambio password" impostata da sistema con cadenza trimestrale.
- ✓ I pc del laboratorio d'informatica sono tutti chromebook e prevedono tutti l'accesso mediante account Google Workspace for Education istituzionale degli alunni.

3.4 E-mail

L'Istituto possiede una casella di posta elettronica istituzionale (@icbusana.edu.it) riservata a personale e studenti e utilizzata per tutte le comunicazioni istituzionali: tale indirizzo e-mail fa parte della Google Workspace for Education.

Agli utenti è fatto divieto di qualsiasi uso della posta elettronica che possa in qualche modo recare danno all'istituto o a terzi e quindi di:

- ✓ prendere visione della posta altrui;
- ✓ simulare l'identità di un altro utente, ovvero utilizzare per l'invio di messaggi credenziali di posta non proprie, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;
- ✓ utilizzare strumenti software o hardware atti ad intercettare il contenuto delle comunicazioni informatiche all'interno dell'istituto;
- ✓ trasmettere a mezzo posta elettronica dati sensibili, personali o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento della protezione dei dati;
- ✓ utilizzare il servizio di posta elettronica per inoltrare contenuti e altre e-mail che non siano di lavoro o a fini di studio.

3.5 Sito web della scuola

Il sito web della scuola è **http://www.icbusana.edu.it** .

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.

Il sito prevede un'area pubblica per le informazioni che non comportano la diffusione di dati personali o riservati, in cui sono reperibili le informazioni sulla vita scolastica, iniziative e scadenze ministeriali, avvisi di carattere generale.

Docenti e genitori possono accedere al sito e consultarlo liberamente.
Per tutte quelle funzioni che implicano l'accesso a informazioni e dati sensibili (Registro elettronico, Aree riservate, etc.).

3.6. Utilizzo di supporti magnetici

Tutto il personale è invitato a non utilizzare dispositivi di memoria esterna (chiavi USB, CD, DVD, ecc.) ma ad utilizzare i Repository su Cloud del dominio @icbusana.edu.it.
Qualora sia indispensabile l'utilizzo di supporti magnetici, gli utenti devono averne particolare cura in particolar modo quelli riutilizzabili, per evitare che persone non autorizzate possano accedere ai dati qui contenuti.
Di conseguenza le azioni da compiere obbligatoriamente sono le seguenti:

- ✓ criptare l'accesso con password sicura
- ✓ custodire i supporti magnetici contenenti dati sensibili e giudiziari in armadi chiusi a chiave onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto;
- ✓ consegnare i supporti magnetici riutilizzabili (DAT, chiavi USB, CD riscrivibili, ...) obsoleti all'Amministratore di sistema per l'opportuna distruzione onde evitare che il loro contenuto possa essere successivamente recuperato in seguito alla cancellazione.

3.7 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).
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 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 19 settembre.
La scuola osserva il rispetto della privacy dei propri utenti e protegge i dati personali che gli stessi conferiscono all'istituto. I dati personali vengono richiesti solo in caso di effettiva necessità e sono trattati in conformità alla normativa vigente (*Decreto legislativo 30 giugno 2003, n. 196,* c.d. Codice della Privacy). L'utente è sempre informato sulle finalità della raccolta dei dati personali al momento della stessa e ne firma, ove necessario, il consenso al trattamento. I dati personali dell'utente non sono comunicati a terzi senza il consenso dello stesso, fatti salvi i casi previsti dalla legge. Se l'utente decide di fornire alla scuola i propri dati personali, la scuola può comunicarli all'interno dell'Istituto o a terzi, che prestano servizi alla scuola, secondo le modalità previste da normativa vigente.

LIBERATORIA PRIVACY

Per le informative legate alla Privacy e le liberatorie per l'utilizzo delle immagini si rimanda alla sezione Privacy del sito di istituto, raggiungibile da questo link:
https://www.icbusana.edu.it/albo-distituto/privacy

3.8 Social Network

La scuola non utilizza Social Network per la didattica.

3.9. BYOD: Regolamento per l'utilizzo dei dispositivi digitali personali a scuola

L'azione del PNSD "Politiche attive per il BYOD" (Bring your own device): letteralmente: "porta il tuo dispositivo" punta a garantire a tutti gli studenti una formazione digitale che parta dal saper usare i propri dispositivi.

Si legge testualmente *"La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficientemente integrato"*. Poiché la tecnologia fornisce agli studenti opportunità innovative ed inedite per incrementare la loro cultura, in linea con quanto specificato nel PNSD, il nostro Istituto intende favorire tale processo garantendone la sicurezza attraverso una modalità di interazione che contribuisca al miglioramento dell'ambiente educativo e di apprendimento.

1. Dispositivi ammessi: notebook con installato il browser Chrome, Chromebook, tablet con installato il browser Chrome, fotocamera digitale, lettori e registratori audio e/o video, smartphone.
2. I dispositivi devono essere usati a scuola per soli scopi didattici e solo dopo previa richiesta e/o autorizzazione esplicita dell'insegnante. Agli studenti non è permesso usarli per giochi o attività diverse da quelle didattiche durante le ore scolastiche o durante le pause ricreative.
3. È vietato agli studenti usare dispositivi di registrazione audio, videocamere o fotocamere (o dispositivi che li prevedano) per registrare media o fare foto in classe.
4. Audio e video registrati a scuola a fini didattici possono essere pubblicati esclusivamente in canali di comunicazione intestati ufficialmente all'I.C. Ariosto.
5. Gli studenti sono responsabili personalmente dei propri dispositivi; è vietato prendere in prestito dispositivi di altri studenti.
6. La scuola non è responsabile della sicurezza dei dispositivi e di eventuali danni.
7. Gli studenti sono responsabili di riportare a casa il dispositivo al termine delle lezioni. La scuola non sarà ritenuta responsabile per nessun dispositivo degli studenti lasciato a scuola.
8. Uso non consentito di Internet:
   - ✓ Usare Internet per scopi diversi da quelli didattici;
   - ✓ Scaricare musica, video e programmi da internet;

- ✓ Giocare sul computer, in rete o diversamente (se non come parte di una lezione);
- ✓ usare dispositivi audio, video o fotografici per ritrarre qualsiasi persona durante l'attività didattica per scopi diversi da quelli didattici.

9. Diritto di ispezione
   - ✓ La scuola si riserva il diritto di monitorare le attività online degli utenti.
   - ✓ La scuola, in accordo con la famiglia, può ispezionare la memoria del dispositivo dello studente se ritiene che le regole scolastiche non siano state rispettate, questo comprende, ma non è limitato, a registrazioni audio e video, fotografie scattate nelle pertinenze scolastiche e che violano la privacy altrui, o ogni altra questione legata a cyberbullismo, ecc.
10. Sanzioni per il mancato rispetto delle regole sopra elencate relative al BYOD

L'accesso al network della scuola è un privilegio, non un diritto. L'uso della tecnologia, sia essa proprietà della scuola o un dispositivo fornito dagli studenti, comporta responsabilità personali. Ci si aspetta che gli studenti rispettino le regole dell'I.C., agiscano responsabilmente e onorino i termini e le condizioni fissate dall'insegnante di classe e dalla scuola. Il mancato rispetto di questi termini e condizioni potrà risultare nella temporanea perdita di accesso alla rete nonché `altre azioni disciplinari e legali, se necessario. Gli studenti saranno ritenuti responsabili delle loro azioni e sono incoraggiati a segnalare immediatamente ogni uso accidentale al loro insegnante. Le sanzioni dipenderanno dalla gravità dell'accaduto e sanzionate secondo il Regolamento di Istituto. I dispositivi potranno essere confiscati per l'intera giornata.

4. STRUMENTAZIONE PERSONALE

Per quanto riguarda la gestione degli strumenti personali (cellulari, tablet, etc.) da parte degli studenti, dei docenti e di tutto il personale della scuola, si rinvia a quanto previsto dal Regolamento d'Istituto e dal Patto di corresponsabilità scuola famiglia nell'integrazione specifica

Per gli studenti: gestione degli strumenti personali: cellulari, tablet, ecc…

In ambito scolastico è consentito l'uso di dispositivi elettronici solo per fini didattici. L'utilizzo dei dispositivi deve essere in ogni caso autorizzato dai docenti.

Al di fuori dell'utilizzo strettamente collegato allo svolgimento delle attività didattiche è vietato l'uso di tutti i dispositivi elettronici compresi i telefoni cellulari ed i dispositivi per ascoltare musica.

Per gli alunni con bisogni educativi speciali (DSA - BES) si adotteranno le modalità di impiego di strumenti compensativi quali tablet e computer portatili previsti all'interno del PDP; gli alunni potranno altresì utilizzare il proprio dispositivo personale.

Per i docenti e il personale della scuola: gestione degli strumenti personali: cellulari, tablet, ecc…

Ogni docente può utilizzare la connessione tramite il pc di classe per la gestione del registro elettronico e per l'attività didattica; alcuni docenti utilizzano propri dispositivi, ma solo a fini didattici.

Telefoni cellulari, tablet, 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.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI

5.1 Rischi

La prima responsabilità degli insegnanti consiste, dunque, nell'imparare a **riconoscere** i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente. Per ogni rischio individuato, sono previste azioni specifiche:

RISCHI	AZIONI
Adescamento online (grooming)	Sensibilizzazione sull'esistenza di individui che usano la rete per instaurare relazioni, virtuali o reali, con minorenni e per indurli alla prostituzione. Qualora si venga a conoscenza di casi simili, occorre valutarne la fondatezza e avvisare il Dirigente Scolastico per l'intervento delle forze dell'ordine.
Cyberbullismo	Campagne di sensibilizzazione e informazione anche con l'ausilio di progetti e realtà esterni. I casi possono essere molto variegati, variando dal semplice scherzo di cattivo gusto via sms/Whatsapp a vere e proprie minacce verbali e fisiche, che costituiscono reato. Occorre confrontarsi con il Dirigente Scolastico sulle azioni da intraprendere.
Dipendenza da Internet, videogiochi,	Informazioni sul fatto che ciò può rappresentare una vera e propria patologia che compromette la salute e le relazioni sociali

shopping o gambling online, ...	e che in taluni casi (per es. uso della carta di credito a insaputa di altri) rappresenta un vero e proprio illecito.
Esposizione a contenuti pornografici, violenti, razzisti, ...	*Verso i genitori*: informazione circa le possibilità di attivare forme di controllo parentale della navigazione e sensibilizzazione sulla necessità di monitorare l'esperienza online dei propri figli. *Verso la componente studentesca*: inserimento nel curricolo di temi legati alla affidabilità delle fonti online, all'interculturalità e al rispetto delle diversità. Qualora si venga a conoscenza di casi simili, occorre convocare i genitori per richiamarli a un maggiore controllo sulla fruizione di Internet da parte dei propri figli e/o sulla necessità di non usufruirne in presenza degli stessi.
Sexting e pedopornografia.	*Verso i genitori:* informazione circa le possibilità di attivare forme di controllo parentale della navigazione. *Verso la componente studentesca:* inserimento nel curricolo di temi legati all'affettività, alla sessualità e alle differenze di genere. In casi simili, se l'entità è lieve occorre in primo luogo parlarne con alunne e alunni e rispettivi genitori, ricordando loro che l'invio e la detenzione di foto che ritraggono minorenni in pose sessualmente esplicite configura il reato di distribuzione di materiale pedopornografico. Chi è immerso dalla nascita nelle nuove tecnologie spesso non è consapevole che una foto o un video diffusi in rete potrebbero non essere tolti mai più né è consapevole di scambiare o diffondere materiale pedopornografico. In casi di rilevante gravità occorre informare tempestivamente il Dirigente Scolastico per gli adempimenti del caso.
Violazione della privacy	Informazione sull'esistenza di leggi in materia di tutela dei dati personali e di organismi per farle rispettare. Se il comportamento rilevato viola solo le norme di buona convivenza civile e di opportunità, occorre convocare i soggetti interessati per informarli e discutere dell'accaduto e concordare forme costruttive ed educative di riparazione. Qualora il comportamento rappresenti un vero e proprio illecito, il Dirigente Scolastico deve esserne informato in quanto a seconda dell'illecito sono previste sanzioni amministrative o penali.

5.2 Sensibilizzazione e prevenzione

Le misure di prevenzione comprendono l'integrazione nel curricolo dei temi legati al corretto utilizzo delle TIC e di Internet. La progettazione di incontri didattici specifici deve essere pianificata, garantendo un intervento su ogni classe, con la presenza del Team digitale o di personale esperto.

La scuola può avvalersi della collaborazione di enti e associazioni per realizzare incontri rivolti alla componente studentesca e alle famiglie con l'intento di fornire ogni elemento utile alla prevenzione e alla gestione dei problemi relativi alla sicurezza informatica.

E' inoltre attivo lo sportello ascolto con la psicologa scolastica.

5.3 Segnalazione

La rilevazione dei casi è compito dell'intera comunità scolastica, secondo la sensibilità di ciascuno e la presenza in particolari momenti o contesti.
La scuola ha in attivo uno sportello di ascolto al quale la componente studentesca si può rivolgere per avere consigli e sostegno psicologico anche relativamente alle tematiche del cyber-bullismo.

E' stato inoltre costituito il Team Emergenza Bullismo e Cyberbullismo con compiti di presa in carico delle segnalazioni e di attivazione delle procedure specifiche di intervento.
Tra gli strumenti di rilevazione si utilizzeranno il diario di bordo e i questionari, i modelli e gli schemi proposti all'interno del progetto Generazioni Connesse https://www.generazioniconnesse.it

Segnalazione da parte del personale

Per le segnalazioni di fatti rilevati sono previsti in particolare i seguenti strumenti che i docenti possono utilizzare sulla base della gravità dell'accaduto:

- ✓ annotazione del comportamento sul registro e comunicazione scritta ai genitori, che la devono restituire vistata;
- ✓ convocazione scritta e colloquio con i genitori degli alunni, da parte dei docenti;
- ✓ relazione scritta al Dirigente scolastico.

In base all'urgenza le comunicazioni formali possono essere precedute da quelle informali, effettuate per le vie brevi.
Per i reati più gravi (es. pedopornografia) l'Istituzione scolastica ha l'obbligo di effettuare la denuncia all'autorità giudiziaria (o più semplicemente agli organi di polizia territorialmente competenti).
Inoltre ci si potrà avvalere dei due servizi messi a disposizione dal Safer Internet Center:

- ✓ "*Clicca e Segnala*" di Telefono Azzurro;
- ✓ "*STOP-IT*" di Save the Children.

Una volta ricevuta la segnalazione, infatti, gli operatori procederanno a coinvolgere le autorità competenti in materia.

Strumenti di segnalazione a disposizione degli studenti

Per aiutare gli studenti 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;
- ✓ docente referente per le segnalazioni (referente bullismo e cyber-bullismo).

Gli studenti si possono inoltre rivolgere ai seguenti servizi:

- ✓ Helpline di Generazioni Connesse (numero verde: 19696)
- ✓ Chat di Telefono Azzurro per supporto ed emergenze: "Clicca e segnala"di Telefono Azzurro;
- ✓ "STOP-IT" di Save the Children Italia per segnalare la presenza di materiale pedopornografico online.

5.4 Gestione dei casi

La gestione dei casi rilevati va differenziata a seconda della loro gravità il primo passo è sempre la condivisione con il DS, il referente bullismo ed il team di emergenza, di ogni episodio rilevato, anche minimo; alcuni casi possono essere affrontati convocando genitori e alunno/a per riflettere insieme su quanto accaduto e decidere in sinergia come intervenire.

Nei casi più gravi e in ogni ipotesi di reato occorre valutare tempestivamente con il Dirigente Scolastico come intervenire.

Ogni volta che un membro del personale o studente viola la E-Safety Policy, la decisione finale sul livello di sanzioni sarà a discrezione del Dirigente Scolastico e rifletterà le procedure comportamentali e disciplinari della scuola.

SERVIZI DI SUPPORTO PRESENTI SUL TERRITORIO

Talvolta nella gestione dei casi sia necessario rivolgersi ad altre figure enti ed 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).

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.

RIFERIMENTI

AZIENDE SANITARIE LOCALI

I riferimenti per contattare le aziende sanitarie della propria città si trovano al seguente link:
http://salute.regione.emilia-romagna.it/ssr/aziende-sanitarie-irccs/erogazione-dellassistenza aziende-sanitarieirccs-asp

Uffici Relazioni col pubblico distrettuali:

URP Arcispedale S. Maria Nuova - urp.santamarianuova@ausl.re.it
Tel. centralino: 0522.335111
URP Reggio Emilia - urp.reggioemilia@ausl.re.it
URP Castelnovo né Monti - urp.castelnovomonti@ausl.re.it
Competenze/Servizi: ottenere un sostegno psicologico, psichiatrico o neuropsichiatrico sulle problematiche psicologiche, anche associate all'uso di Internet e a tutti i tipi di comportamenti a rischio e che configurino un reato.

GARANTE REGIONALE PER L'INFANZIA E L'ADOLESCENZA

Viale Aldo Moro, 50 40127 Bologna, tel. 051. 5276263 - 051. 5275713

garanteinfanzia@regione.emilia-romagna.it

www.assemblea.emr.it/garanti/attivita-e-servizi/infanzia

Competenze/Servizi: segnala all'autorità giudiziaria i servizi sociali e competenti; accoglie le segnalazioni di presunti abusi; fornisce informazioni sulle modalità di tutela e di esercizio di questi diritti; segnala alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate, sempre per tutti i comportamenti a rischio e che configurino un reato.

UFFICIO SCOLASTICO REGIONALE

Via de' Castagnoli, 1 40126 – Bologna. Tel: 051. 37851

direzione-emiliaromagna@istruzione.it

www.istruzioneer.it/

Competenze/Servizi: tra le varie funzioni, supporta la scuola in attività di prevenzione. Può affiancare le scuole nei casi di segnalazione di comportamenti a rischio correlati all'uso di internet e per i comportamenti a rischio e che configurino un reato relativi al cyberbullismo.

TRIBUNALE PER I MINORENNI

Via del Pratello, 36 40122 – Bologna. Tel: 051. 2964880

tribmin.bologna@giustizia.it

http://www.tribmin.bologna.giustizia.it/

Competenze/Servizi: tra le varie attività si occupa di tutti i procedimenti che riguardano reati, misure rieducative, tutela e assistenza, sempre per tutti i comportamenti a rischio e che configurino un reato.

POLIZIA POSTALE E DELLE COMUNICAZIONI

Via Francesco Zanardi, 28/6 – Bologna. Tel: 051. 6352611

poltel.bo@poliziadistato.it

www.commissariatodips.it/

Competenze/Servizi: si occupa di accogliere tutte le segnalazioni o denunce relative a comportamenti a rischio nell'utilizzo di internet sempre per tutti i comportamenti a rischio e che configurino un reato, quali: furto di identità, cyberbullismo (nel caso di cyberstalking), commercio on-line (nel caso di clonazione di carta di credito), pedopornografia on-line, grooming (adescamento on-line), gioco d'azzardo on-line, sexting.

Procedure di gestione dei casi

Per tutte le procedure specifiche si rimanda agli allegati in calce.

6. ALLEGATI

Allegato 1: Segnalazione dei casi

MODULO PER LA SEGNALAZIONE DI CASI

ISTITUTO COMPRENSIVO DI SCUOLA INFANZIA PRIMARIA SECONDARIA 1°GR.
"L. ARIOSTO" VIA SASSO, 3 42032 BUSANA (RE)
c.f. 80016110357 tel. 0522/891150 WWW.ICBUSANA.EDU.IT
e-mail: segreteria@icbusana.edu.it pec: reic81600g@pec.istruzione.it

Descrizione dell'episodio o del problema		
Soggetti coinvolti	Vittima/e:	Classe:
	1.	
	2.	
	3.	
	Bullo/i:	Classe:
	1.	
	2.	
	3.	
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 il bullo? 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:	

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:

Allegato 2: Diario di bordo

Utilizzare il **diario di bordo** per tenere traccia di ciò che è avvenuto rispetto ai comportamenti degli alunni online e di come è stato gestito.

Co-financed by the European Union
Connecting Europe Facility

Generazioni Connesse

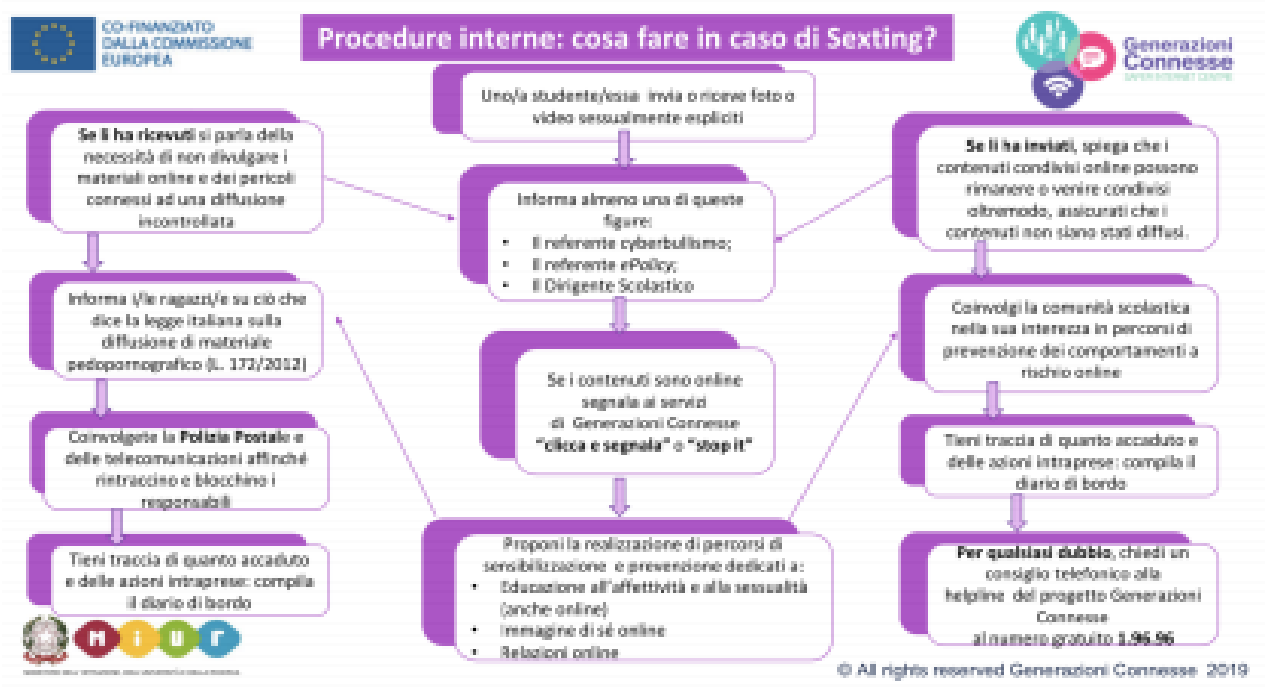
Schema riepilogativo delle situazioni gestite legate a rischi online

Riepilogo casi
Scuola_____ Anno Scolastico_____

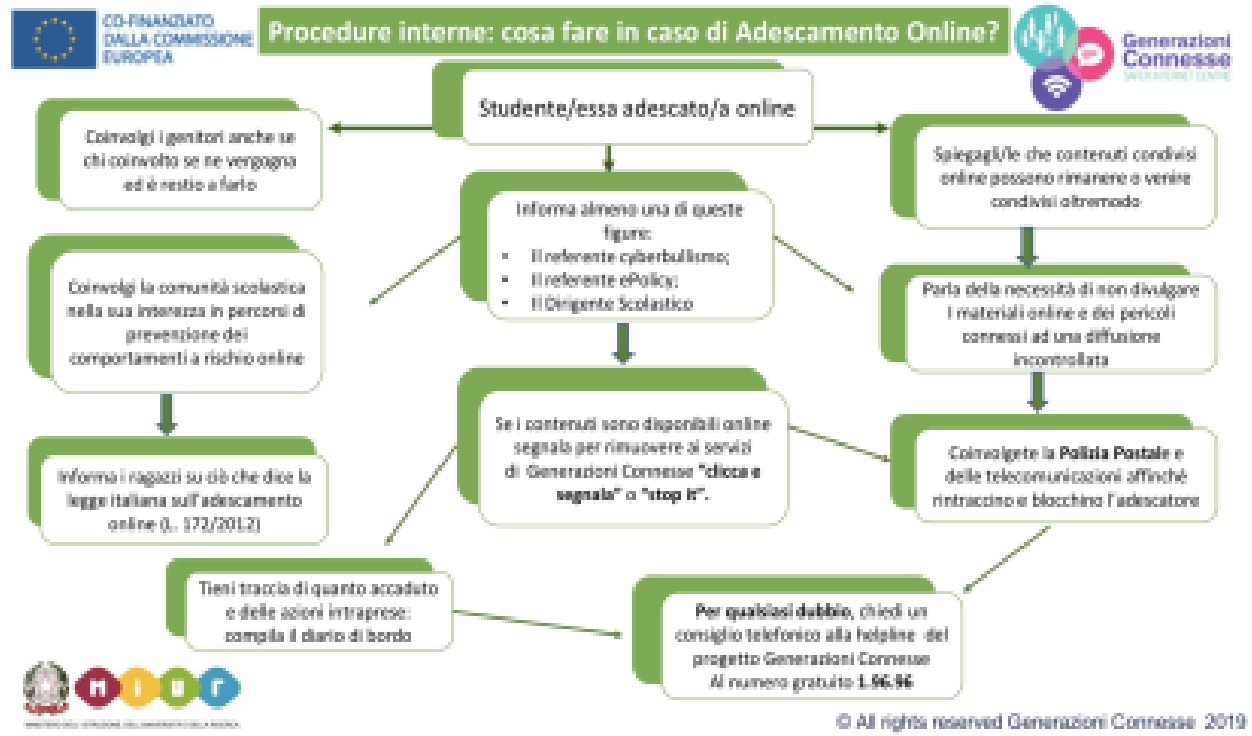
N°	Data	ora	Episodio *(riassunto)*	Azioni intraprese		Insegnante con cui l'alunno/a si è confidato	Firma
				Cosa?	Da chi?		

Allegato 3: Schema di intervento in caso di Cyberbullismo

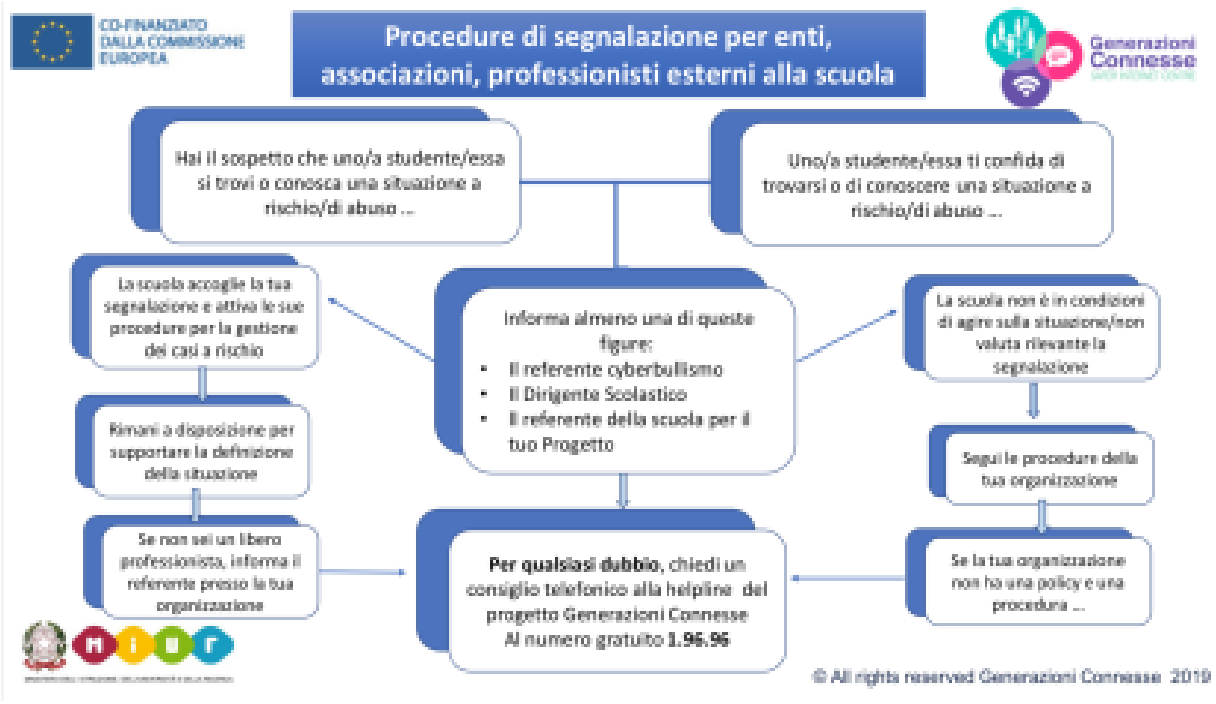
Allegato 4: Schema di intervento in caso di Sexting



Allegato 5: Schema di intervento in caso di Adescamento Online



Allegato 6: Procedure di segnalazione per enti, associazioni, professionisti esterni alla scuola



Allegato 7: Modello di segnalazione al garante

Modello da compilare per la segnalazione al garante si può scaricare al seguente indirizzo: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6732688

Allegato 8: Linee guida per i ragazzi

LINEE GUIDA PER I RAGAZZI

1. **FAI ATTENZIONE** perché rimane sempre traccia di quello che posti o scrivi su internet;
2. **STAI ATTENTO** a chi vuol sapere troppe cose. Non dare a nessuno informazioni personali e della famiglia (nome, cognome, età, indirizzo, numero di telefono, nome e orari della scuola, nome degli amici).
3. **CHIEDI SEMPRE IL PERMESSO** prima di inviare o pubblicare su una chat , un social o su una app, qualsiasi materiale in cui ci siano altre persone (foto, video, commenti, etc.) ;
4. **CHIEDITI** se vorresti esserci tu al suo posto quando fai commenti, metti foto o video di/su altri.
5. **NON RISPONDERE alle offese** ed agli insulti;
6. **CONSERVA E SALVA le comunicazioni offensive**, ti potrebbero essere utili per dimostrare quanto ti è accaduto;
7. Se ricevi materiale offensivo (e-mail, sms, mms, video, foto, messaggi vocali) **NON DIFFONDERLO**: potresti essere accusato di cyberbullismo;
8. Rifletti prima di inviare: ricordati che tutto ciò che invii **su internet** diviene pubblico e **rimane per SEMPRE**;
9. Quando sei connessi alla rete **RISPETTA SEMPRE GLI ALTRI,** ciò che per te è un gioco può rivelarsi offensivo per qualcun altro;
10. SE PARTECIPI A GRUPPI in cui leggi offese, dillo ai tuoi genitori o insegnanti, fai screenshot, salva il materiale e poi esci dal gruppo.
11. **Riferisci al tuo insegnante o ai tuoi genitori** se qualcuno ti invia immagini che ti infastidiscono e non rispondere; riferisci anche al tuo insegnante o ai tuoi genitori se ti capita di trovare immagini di questo tipo su Internet;
12. Ricordati che se qualcuno ti offende pesantemente puoi ricorrere alla Dirigente, al referente bullismo, ai tuoi genitori e anche alla Polizia postale
13. Ricordati che **è facile mentire su internet.** Alcune persone possono fingersi per quello che non sono. Anche le immagini web possono essere false.
14. **PENSA** prima di mettere qualsiasi cosa su internet. NON pubblicare, inviare o condividere materiale imbarazzante o dannoso e inopportuno.
15. Tutti quelli che osservano senza far nulla diventano **corresponsabili delle azioni** del cyber bullo; mettere un “like” su un social o condividere o commentare foto o video sottopone chi lo fa a una responsabilità maggiore.
16. **Rispettate la privacy altrui.** State attenti soprattutto a non pubblicare informazioni personali relative ad altri (comprese immagini, foto o video) senza il loro consenso.
17. La privacy non vi protegge se commettete atti di cybebullismo su qualcuno (offese, messaggio volgari, foto private e intime etc.).
18. Utilizza password sicure (lunghe con numeri e lettere) tienile riservate. Se vedi cose strane cambiale.
19. **Non scaricare** - senza parlarne con gli adulti - loghi, suonerie, app, immagini o file in genere, sia da Internet che come allegati a messaggi di posta elettronica, che possono creare intromissioni nel computer, ovvero possono comportare costi o addebiti indesiderati.

Allegato 9: Linee guida per i genitori

LINEE GUIDA PER I GENITORI

Consigli per difendere i propri figli dai pericoli legati all'uso delle nuove tecnologie Molti bambini utilizzano internet già durante i primi anni della scuola primaria (6-7 anni). È importante sottolineare che è fondamentale l'accompagnamento all'utilizzo di internet da parte di un adulto (genitore, insegnante, educatore) in relazione all'età del bambino.

I bambini al di sotto dei 10-11 anni, in genere, non avendo ancora sviluppato le capacità di pensiero critico necessarie, non sono in grado di esplorare il web da soli. Scaricano musica, utilizzano motori di ricerca per trovare informazioni, visitano siti, inviano e ricevono sms, la posta elettronica e i giochi online. La supervisione degli adulti è quindi fondamentale anche in questa fase, poiché una maggior conoscenza e consapevolezza legate alla crescita non mettono comunque al riparo dai rischi della Rete.

- ✓ Chiedete ai vostri figli di essere informati rispetto alla loro attività in rete: cosa fanno e con chi stanno condividendo;
- ✓ Ricordatevi che siete responsabili fino ai 14 anni dell'utilizzo che fanno del loro smartphone;
- ✓ Utilizzate app di condivisione (tipo whatsapp) tra genitori in modo consono allo scopo per cui vengono creati i gruppi, utilizzando modalità comunivative appropriate;
- ✓ Stabilite i tempi di utilizzo del computer e del collegamento in rete secondo l'età del minore;
- ✓ Condividete con lui le raccomandazioni e le regole di utilizzo dello smartphone per un uso consapevole e corretto;
- ✓ Creare un rapporto di dialogo con il minore, essere disponibili, farsi raccontare dei suoi contatti e dei suoi interessi in rete (siti visitati, chat, ricerche e scoperte effettuate);
- ✓ Di tanto in tanto controllare i contenuti postati su Internet dai vostri figli.;
- ✓ Non lasciare da soli i ragazzi nell'utilizzo dello smartphone, soprattutto se frequentano la primaria
- ✓ Fate in modo di non lasciare a loro disposizione lo smartphone di notte;
- ✓ Utilizzate applicativi che possano aiutarvi nel controllo dello smartphone;
- ✓ Parlate apertamente dei rischi che si possono correre utilizzando internet e whatsapp;
- ✓ Controllate la cronologia o gli applicativi scaricati sul loro smartphone;
- ✓ Dite di non dare mai dati personali in rete;
- ✓ Ditegli di non rispondere agli insulti perché così diventa anche lui colpevole;
- ✓ Ricordagli che tutti i cellulari o pc lasciano una traccia che può essere trovata dalla Polizia;
- ✓ Ricordargli che le cose scritte o alcune fotografie, POSSONO FAR PIU' MALE perché rimangono SEMPRE;
- ✓ Fate presente che molti comportamenti illeciti che loro conosco nel reale (insultare, offendere , fotografare di nascosto, accedere illecitamente ad un servizio, etc.) lo sono anche nel virtuale;
- ✓ Fate presente e insistete che qualcosa messo su internet è incancellabile;
- ✓ Salvate sul computer il materiale che può fungere da prova (per esempio screenshot, conversazioni in chat e immagini) e subito dopo, se possibile, cancellare – o far cancellare dal gestore della piattaforma – tutti i contenuti in rete;
- ✓ Se sono coinvolti compagni di scuola, i genitori dovrebbero rivolgersi agli insegnanti e, laddove presente, allo psicologo scolastico per valutare se sporgere denuncia presso la polizia.

LINK UTILI

- ✓ www.commissariatops.it
- ✓ www.generazioniconnesse.it