ISTITUTO COMPRENSIVO STATALE
"AUGUSTA BAGIENNORUM"
BENE VAGIENNA
Viale Rimembranza, 2
12041 BENE VAGIENNA CN
Tel.0172 654118- fax 0172654934
segreteria@icbenevagienna.it
cnic80700n@pec.istruzione.it

LINEE GUIDA PER UNA E-Safety Policy

1 Introduzione

1.1. Scopo della Policy

L'e-policy è il documento programmatico della politica per la sicurezza informatica dell'Istituto Comprensivo di Bene Vagienna. Si applica a tutti i soggetti della comunità scolastica (studenti, famiglie, insegnanti, personale ATA) e ad ogni frequentatore esterno occasionale (esperti, tecnici…).

La presenza sempre più diffusa delle tecnologie digitali offre grandi opportunità di crescita e apprendimento. Tuttavia impone una regolamentazione per un uso efficace e sicuro. E' infatti di fondamentale importanza sia la sicurezza che riguarda la protezione dei dati (privacy) e dei dispositivi sia la tutela degli studenti attraverso la prevenzione e il contrasto a fenomeni di cyberbullismo che possano minare la serenità e la salute dei ragazzi.

Per gli studenti e per gli insegnanti l'accesso ad internet è un privilegio e un diritto.
I docenti hanno la responsabilità di guidare gli studenti nelle attività on-line, di stabilire obiettivi chiari per un uso responsabile di internet.
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.

Il presente documento ha lo scopo di descrivere le norme comportamentali e le procedure per l'utilizzo delle ICT nell'Istituto Comprensivo "*Augusta Bagiennorum*", le misure per la prevenzione e quelle per la rilevazione e gestione delle problematiche connesse a un uso non consapevole delle tecnologie digitali.

In particolare, le finalità dell'Istituto sono:
a) promuovere l'educazione all'uso consapevole della rete internet e l'educazione ai diritti e ai doveri legati all'utilizzo delle tecnologie informatiche
b) prevenire fenomeni legati ai rischi delle tecnologie digitali;

c) segnalare i casi individuati all'interno della scuola;
d) gestire i casi, ovvero le misure che la scuola intende attivare a supporto delle famiglie e degli studenti che sono stati vittime o spettatori attivi e/o passivi di quanto avvenuto.

Il nostro Istituto a tutela della privacy dei propri utenti si impegna a proteggere i dati personali in conformità alla normativa vigente.
Relativamente alla tutela della persona ed di altri soggetti, rispetto al trattamento dei dati personali la titolarità è esercitata dal Dirigente Scolastico.
Il Dirigente Scolastico designa il responsabile del trattamento dei dati, che coincide con la figura del Direttore DSGA.
Ai genitori e/o agli esercenti della responsabilità genitoriale è richiesta all'inizio dell'anno scolastico un'autorizzazione alla pubblicazione della documentazione multimediale, da utilizzare a scopo documentario, didattico e senza fini di lucro.
E' diritto dei genitori o esercenti della responsabilità genitoriale rifiutare tale autorizzazione.

Il monitoraggio e l'implementazione della e-policy verranno curati dal Dirigente scolastico in collaborazione con l'Animatore Digitale e il Referente per il Cyberbullismo con il supporto dello staff di Generazioni Connesse cui l'Istituto farà riferimento.

1.2. Ruoli e responsabilità

1. Il Dirigente scolastico cura la sicurezza on-line della comunità scolastica:
   - favorisce la cultura dell'inclusione dell'altra/o 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.
   - garantisce la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
   - garantisce ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (ITC) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
   - garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line;
   - deve informare tempestivamente, qualora venga a conoscenza di atti di cyberbullismo che non si configurino come reato, i genitori dei minori coinvolti (o chi ne esercita la responsabilità genitoriale o i tutori);
   - Il dirigente Scolastico regola il comportamento degli studenti ed impone sanzioni disciplinari in caso di comportamento inadeguato.

2. Animatore Digitale:

   - **Formazione interna**: stimola la formazione interna alla scuola negli ambiti del Piano

Nazionale Scuola Digitale (PNSD), attraverso l'organizzazione di laboratori formativi (senza essere necessariamente un formatore), favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative, come ad esempio quelle organizzate attraverso gli snodi formativi;

- **Coinvolgimento della comunità scolastica**: favorisce la partecipazione e stimola il protagonismo degli studenti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, anche attraverso momenti formativi aperti alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa;
- **Creazione di soluzioni innovative**: individua soluzioni metodologiche e tecnologiche sostenibili da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; la pratica di una metodologia comune; informazione su innovazioni esistenti in altre scuole; un laboratorio di coding per tutti gli studenti), coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure.

L'animatore si trova a **collaborare con l'intero staff della scuol**a e in particolare con gruppi di lavoro, operatori della scuola, dirigente, DSGA, soggetti rilevanti, anche esterni alla scuola, che possono contribuire alla realizzazione degli obiettivi del PNSD. Può, e dovrebbe, inoltre, coordinarsi **con altri animatori digitali sul territorio**, per la creazione di gruppi di lavoro specifici.

3. Referente per il Cyberbullismo d'Istituto:
   - "Coordina le iniziative di prevenzione e di contrasto del bullismo e del cyberbullismo previste dal Piano Triennale dell'Offerta Formativa, avvalendosi della collaborazione delle Forze di Polizia, Carabinieri, e di associazioni e centri di aggregazione giovanili presenti sul territorio."
   - Facilita la formazione e la consulenza di tutto il personale.
   - supporta il Dirigente Scolastico nella revisione/stesura di Regolamenti e atti di Istituto per quanto concerne le misure dedicate alla prevenzione del bullismo e del cyberbullismo.

4. Insegnanti:
   - provvedono personalmente alla propria formazione/aggiornamento sull'utilizzo del digitale con particolare riferimento alla dimensione etica (tutela della privacy, rispetto dei diritti intellettuali dei materiali reperiti in Internet e dell'immagine degli altri: lotta al cyberbullismo);
   - supportano gli alunni nell'utilizzo consapevole delle tecnologie informatiche utilizzate a scopi didattici;
   - segnalano al Dirigente scolastico e ai suoi collaboratori episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni;
   - Supportano ed indirizzano alunni coinvolti in problematiche legate alla rete.

5. Alunni (in considerazione dell'età):

- leggono comprendono ed accettano il documento di E-Safety Policy;
- comprendono e rispettano le norme sul diritto d'autore;
- devono avere consapevolezza delle situazioni di rischio legate alla rete, nell'utilizzo dei dispositivi digitali (telefoni cellulari, computer,, fotocamere digitali);
- devono conoscere la politica della scuola sull'uso delle immagini;
- comprendono l'importanza di adottare buone pratiche di sicurezza on-line quando si usano le tecnologie;
- si assumono la responsabilità di un utilizzo sbagliato delle tecnologie.

6. Responsabile informatico di plesso:
   - è l'unico a poter installare nuovi software;
   - predispone la prenotazione dei laboratori che consente di tenere traccia di ora e laboratorio utilizzati da ciascuno.

7. Personale ATA:

   - Conosce le questioni di sicurezza informatica e la politica dell'Istituto e le relative buone pratiche.
   - Conosce il documento di e-policy;
   - segnala qualsiasi infrazione al regolamento al Dirigente Scolastico o ai suoi collaboratori o all'Animatore Digitale

8. Direttore dei Servizi Generali e Amministrativi:

   - assicura, gli interventi di manutenzione necessari ad evitare un cattivo funzionamento della dotazione tecnologica dell'Istituto, controllando con la consulenza e la super visione del DPO, Avv. Carazza che le norme minime di sicurezza vengano rispettate.

8. Genitori:

   - contribuiscono, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
   - vigilano sull'impiego delle ICT da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
   - agiscono in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite;
   - rispondono per gli episodi commessi dai figli minori a titolo di *culpa in educando* (art. 2048 del Codice civile).

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

Condivisione e comunicazione della Policy ad alunni, personale e genitori attraverso il sito della scuola.

1.4. Gestione delle infrazioni alla Policy.

Salvo che il fatto non costituisca reato (e dunque debba essere denunciato agli Organi competenti avvisata la Dirigente scolastica), i provvedimenti disciplinari nei confronti dell'alunno che ha commesso infrazione alla policy sono presenti nella Sezione XI del Regolamento di Istituto (e in allegato a questo documento).

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

Il monitoraggio della Policy avrà cadenza annuale a cura del Dirigente scolastico e del referente d'Istituto. Ogni eventuale aggiornamento avverrà sulla base di casi problematici riscontrati e della loro gestione e sul riscontro di questionari somministrati ad alunni e docenti atti a verificare l'insorgenza di nuove necessità e la revisione di tecnologie esistenti.

1.6. Integrazione della Policy con Regolamenti esistenti.

Il presente documento si integra per obiettivi e contenuti con i seguenti documenti che specificano le politiche dell'Istituto per un uso efficace e consapevole del digitale nella didattica:

- PTOF, incluso il piano per l'attuazione del PNSD;
- Regolamento interno d'istituto;
- Regolamento per l'utilizzo dei laboratori di informatica.

2 Formazione e Curricolo

2.1 Curricolo sulle competenze digitali per gli studenti

Nell'ambito del PNSD l'Istituto si propone un programma di educazione alla sicurezza on-line da affiancarsi ad una didattica digitale. La scuola si preoccupa pertanto di promuovere una serie di comportamenti "adeguati":

- Appurare l'attendibilità delle informazioni trovate in rete;
- Riportare sempre la fonte delle informazioni pervenute;
- Conoscere e rispettare la netiquette (regole condivise che disciplinano il rapporto tra utenti della rete, siti e qualsiasi altro tipo di comunicazione);
- Mantenere private le informazioni personali proprie e degli altri;
- Comprendere che le fotografie in rete possono essere manipolate o utilizzate per scopi diversi da quelli per cui sono state pubblicate;
- Comprendere che la rete traccia e tiene memoria di tutto ciò che viene pubblicato;
- Comprendere il motivo per cui non bisogna pubblicare foto o video di altre persone senza il loro consenso;
- Conoscere le conseguenze di azioni sbagliate in rete;
- Conoscere le diverse forme di cyberbullismo e le persone e/o associazioni a cui rivolgersi per chiedere consiglio;
- Rispettare i copyright.

2.2 Formazione dei docenti sull'utilizzo consapevole e l'integrazione delle TIC nella

didattica

Le attività di formazione si svolgeranno su diversi livelli:

- formazione istituzionale, organizzata dal Miur secondo il PNSD, attraverso gli snodi formativi;
- formazione istituzionale in contrasto al bullismo, organizzata dal MIUR (Piattaforma Elisa, Generazioni Connesse, altra formazione organizzata dagli Uffici Scolastici):
  - interventi su classi individuate dalla scuola stessa,
  - interventi che vedono la presenza dell'intera comunità educante, compresi i genitori,
  - la formazione dei referenti di istituto;
- formazione specifica di Istituto, legata alle esigenza formative rilevate;

2.3 Sensibilizzazione delle famiglie

Il presente documento verrà pubblicato sul sito ed affiancato da un vademecum per i genitori affinché comprendano i rischi della rete e collaborino proficuamente con il personale della scuola.

Seguire a tal proposito i consigli presenti nel sito Generazioni Connesse (www.generazioniconnesse.it) curato dal Miur e cofinanziato dall'Unione Europea.

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

Si veda in allegato.

3.3 Sito web della scuola

La scuola ha un sito web nel quale sono pubblicati tutti i documenti relativi la sicurezza in rete e la prevenzione di rischi legati ad un uso inconsapevole o sbagliato della stessa.

4 Strumentazione personale

Si rimanda al Regolamento di Istituto (sezione XI) allegato.

5 Prevenzione, rilevazione e gestione dei casi

5.1 Prevenzione

- **Rischi**: La prima responsabilità degli insegnanti consiste nell'imparare a riconoscere i rischi più comuni che i ragazzi possono correre sul web, per potere poi intervenire adeguatamente.

I ragazzi nativi digitali pur essendo spesso tecnicamente competenti, tendono a non cogliere le implicazioni dei loro comportamenti
Ciò fa sì che alcuni rischi che fanno parte del mondo digitale possano non essere percepiti come tali ed è dunque compito degli adulti, famiglie ed insegnanti, affrontarli con l'obiettivo di prevenirli.
Tra i principali rischi, ricordiamo:

- possibile esposizione a contenuti violenti e non adatti alla loro età;
- videogiochi diseducativi;
- pubblicità ingannevoli;
- possibili contatti con adulti che vogliono conoscere e avvicinare bambini/e o ragazzi/e (adescamento);
- rischio di molestie o maltrattamenti da coetanei (cyber-bullismo);
- scambio di materiale a sfondo sessuale (sexting);
- uso eccessivo di Internet/cellulare (dipendenza).

▪ **Azioni:** L'obiettivo che l'insegnante deve proporsi dopo avere riconosciuto il pericolo è non ignorare la richiesta d'aiuto con azioni di contrasto efficaci e mirate, rispetto ai rischi sopra elencati. Tra le azioni utili a contrastare i rischi derivanti da un utilizzo improprio dei dispositivi digitali da parte degli studenti in orario scolastico, vi sono le seguenti:

- diffondere un'informazione capillare rivolta al personale scolastico, agli studenti e alle famiglie, sui rischi che i minori possono correre sul web;
- far rispettare il divieto di utilizzo di dispositivi digitali propri, quali cellulare e smartphone, agli studenti in orario scolastico. Le dovute eccezioni (uso del cellulare per comunicazioni alunno-famiglia in occasione di uscite didattiche) andranno espressamente regolamentate e dovranno comunque avvenire sotto la supervisione diretta di un docente responsabile;
- dotare i dispositivi della scuola di filtri che impediscano l'accesso a siti web non adatti ai minori (black list).

5.2 Rilevazione

Tra i contenuti andranno opportunamente segnalati:

− dati particolari o riservati pubblicati in chat o social network (foto, immagini, video personali, informazioni private proprie o di amici; l'indirizzo di casa o il telefono, ecc.);

− contenuti che possano considerarsi in qualche modo lesivi dell'immagine altrui (commenti offensivi, minacce, osservazioni diffamatorie o discriminatorie, foto o video denigratori, videogiochi che contengano un'istigazione alla violenza, ecc.);

− contenuti riconducibili alla sfera sessuale: messaggi, immagini o video a sfondo sessuale,

Compito del Docente:

− Informare il Dirigente scolastico, il referente d'istituto e le famiglie coinvolte in merito all'accaduto. Sarà il Dirigente scolastico, eventualmente, ad avvisare la Polizia Postale.

Compito del Referente d'istituto:

− Compilazione del modulo in allegato per tenere traccia di tutte le segnalazioni e qualora sia necessario e in accordo con il Dirigente scolastico, chiedere supporto alle Associazioni territoriali o alla Polizia Postale.

AZIONI DA INTRAPRENDERE NEL CORSO DELL'A.S. 2019-2020:

- Architettura rete wifi
- Regolamento per l'accesso al sistema Wi-Fi d'Istituto (da modificare)
- Sezione XI del Regolamento di Istituto "Uso cellulare e dispositivi da parte di studenti, personale e genitori"
- Prenotazione e utilizzo dei laboratori di informatica (da modificare)
- Procedure operative per la gestione delle infrazioni alla Policy (da implementare)
- Tabella per le Segnalazioni dei casi (da implementare)
- Consigli (vademecum) per i genitori (da implementare)
- Legge regionale 32/2018
- Legge nazionale 71/2017
- Linee guida MIUR 2015

Documento approvato nel Collegio docenti del 28 ottobre 2019
e nel Consiglio d'Istituto del 29 ottobre 2019