Ist.Compr. "G.M. GISELLU"- DORGALI
Prot. 0008594 del 29/11/2021
04-05 (Uscita)

Documento di ePolicy

NUIC871007

DORGALI - "G.M. GISELLU"

VIA LAMARMORA 56 - 08022 - DORGALI - NUORO (NU)

Dirigente Scolastico: prof.ssa Marina Cei

Capitolo 1 - Introduzione al documento di ePolicy

1.1 - Scopo dell'ePolicy

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

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

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

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

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

Argomenti del Documento

1. **Presentazione dell'ePolicy**
    1. Scopo dell'ePolicy
    2. Ruoli e responsabilità
    3. Un'informativa per i soggetti esterni che erogano attività educative nell'Istituto
    4. Condivisione e comunicazione dell'ePolicy all'intera comunità scolastica
    5. Gestione delle infrazioni alla ePolicy
    6. Integrazione dell'ePolicy con regolamenti esistenti
    7. Monitoraggio dell'implementazione dell'ePolicy e suo aggiornamento
2. **Formazione e curricolo**
    1. Curricolo sulle competenze digitali per gli studenti
    2. Formazione dei docenti sull'utilizzo e l'integrazione delle TIC (Tecnologie dell'Informazione e della Comunicazione) nella didattica
    3. Formazione dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali
    4. Sensibilizzazione delle famiglie e Patto di corresponsabilità
3. **Gestione dell'infrastruttura e della strumentazione ICT (Information and Communication Technology) della e nella scuola**
    1. Protezione dei dati personali
    2. Accesso ad Internet
    3. Strumenti di comunicazione online
    4. Strumentazione personale
4. **Rischi on line: conoscere, prevenire e rilevare**
    1. Sensibilizzazione e prevenzione
    2. Cyberbullismo: che cos'è e come prevenirlo
    3. Hate speech: che cos'è e come prevenirlo
    4. Dipendenza da Internet e gioco online
    5. Sexting
    6. Adescamento online
    7. Pedopornografia
5. **Segnalazione e gestione dei casi**
    1. Cosa segnalare
    2. Come segnalare: quali strumenti e a chi
    3. Gli attori sul territorio per intervenire
    4. Allegati con le procedure

Perché è importante dotarsi di una E-policy?

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

all'uso di Internet.

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

Il documento E-policy ha l'obiettivo di promuovere una visione educativa e una proposta formativa attente ad un uso corretto e responsabile delle tecnologie digitali, delle strumentazioni informatiche collegate al web del nostro Istituto e a disposizione dei docenti e degli alunni, nel rispetto della normativa vigente.

All'interno del presente documento saranno contenute:

- le misure atte a facilitare e promuovere l'utilizzo delle TIC nella didattica;
- le misure di prevenzione di un uso improprio della rete;
- le misure di segnalazione di eventuali casi di: cyberbullismo, sexting, adescamento online, dipendenza da internet e giochi online, hate speech;
- le misure per la gestione dei casi.

1.2 - Ruoli e responsabilità

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

Il Dirigente Scolastico

- ha il compito di garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- promuove la cultura della sicurezza online;
- garantisce ai propri docenti una formazione di base sulle Tecnologie dell'Informazione e della Comunicazione (TIC) che consenta loro di possedere le competenze necessarie all'utilizzo di tali risorse;
- fornisce il proprio contributo all'organizzazione, insieme al docente referente sulle tematiche del bullismo/cyberbullismo, di corsi di formazione specifici per tutte le figure scolastiche sull'utilizzo positivo e responsabile delle TIC;
- gestisce ed interviene nei casi di bullismo, cyberbullismo e uso improprio delle tecnologie digitali.

L'Animatore digitale in collaborazione con il Team digitale

- supporta il Personale Scolastico da un punto di vista non solo tecnico-informatico, ma anche in riferimento ai rischi online, alla protezione e gestione dei dati personali;
- promuove percorsi di formazione interna all'Istituto negli ambiti di sviluppo della "scuola digitale" (con riferimento, ad esempio, alle competenze digitali previste anche per l'educazione civica);
- monitora e rileva eventuali episodi o problematiche connesse all'uso delle TIC a scuola;
- ha il compito di controllare che gli utenti autorizzati accedano alla Rete della scuola con apposita password, per scopi istituzionali e consentiti (istruzione e formazione).

Il Referente bullismo e cyberbullismo

- coordina e promuove iniziative specifiche per la prevenzione e il contrasto del bullismo e del cyberbullismo, avvalendosi anche della collaborazione delle Forze di polizia, delle associazioni e degli enti territoriali;
- ove possibile coinvolge, con progetti e percorsi formativi ad hoc, studenti, colleghi e genitori.

I Docenti

- hanno un ruolo centrale nel diffondere la cultura dell'uso responsabile delle TIC e della Rete;
- integrano parti del curriculum della propria disciplina con approfondimenti sull'uso responsabile delle TIC e della Rete, promuovendo, laddove possibile, anche l'uso delle tecnologie digitali nella didattica;
- accompagnano e supportano gli studenti e le studentesse nelle attività di apprendimento e nei laboratori che prevedono l'uso della LIM o di altri dispositivi tecnologici che si connettono alla Rete;
- hanno il dovere morale e professionale di segnalare al Dirigente Scolastico qualunque problematica, violazione o abuso, anche online, che vede coinvolti studenti e studentesse in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalla normativa;
- si informano e/o 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;
- si assicurano che gli alunni conoscano e utilizzino in modo critico le opportunità di ricerca offerte dalle tecnologie digitali e dalla rete e li guidano alla navigazione sicura;
- assicurano la riservatezza dei dati personali trattati ai sensi della normativa vigente;
- controllano l'uso delle tecnologie digitali/ dispositivi mobili, da parte degli alunni durante le lezioni e ogni altra attività scolastica (se consentito);

- comunicano ai genitori difficoltà, problematiche rilevate a scuola e connesse all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo;
- segnalano qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore digitale/team digitale al fine di ricercare soluzioni metodologiche e tecnologiche innovative da diffondere nella scuola e si aggiornano sulla politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC.

Studenti e studentesse

- devono assumere un atteggiamento responsabile nell'utilizzo delle TIC;
- devono conoscere le potenzialità offerte dalle TIC per la ricerca/rielaborazione di contenuti e materiali;
- devono comprendere l'importanza di adottare buone pratiche di sicurezza online quando si utilizzano le tecnologie digitali, in modo da prevenire eventuali rischi;
- devono adottare condotte rispettose degli altri anche quando si comunica in rete;
- devono poter esprimere dubbi/ difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

Genitori

- sostengono la linea di condotta adottata dalla scuola nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- incoraggiano gli alunni e le alunne nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti;
- concordano con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati nell' uso non responsabile o pericoloso delle tecnologie digitali o di internet.
- monitorano l'utilizzo a casa degli strumenti digitali e di internet.

Il Direttore dei Servizi Generali e Amministrativi

- assicura, nei limiti delle risorse finanziarie disponibili, gli interventi di manutenzione richiesti da cattivo funzionamento e/o danneggiamento della dotazione tecnologica dell'Istituto, controllando al contempo che le norme di sicurezza vengano rispettate;
- facilita la trasmissione di comunicazioni relative alle tecnologie digitali tra le varie componenti della scuola (Dirigente Scolastico, Animatore digitale, docenti e famiglie degli alunni);
- cura la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dall'Animatore digitale, dal Tecnico informatico, dal Team digitale, provvedendo all'intervento del personale tecnico di assistenza.

Il Tecnico informatico

- Può controllare e accedere a tutti i file della intranet;
- si occupa dell'installazione di nuovi software;
- si occupa della manutenzione dei dispositivi in dotazione al nostro Istituto.

Il Data Protection Officer

Ai sensi del Nuovo Regolamento Europeo sulla privacy 679/2016 è stato conferito incarico di DPO ad un professionista esterno alla scuola i cui contatti sono reperibili sul sito della scuola alla apposita sezione dedicata alla privacy. In particolare in DPO si occupa di:

- fornire consulenza al responsabile della conservazione dei dati personali e di informare tutte le figure coinvolte, sia in merito alla normativa, sia riguardo alle soluzioni tecniche adottate per rispettare gli standard imposti;
- analizzare i meccanismi di raccolta e conservazione dei dati in atto;
- produrre un documento in cui si evidenziano eventuali necessità di adeguamento tecnologico o di correttivi da apportare alle procedure in atto;
- redigere un piano di aggiornamento e manutenzione dei sistemi in linea con l'evolversi della normativa in materia.
- interfacciarsi con le autorità di controllo, per tutte le questioni che riguardano la consultazione preventiva, la possibilità di reperire i dati anche in caso di guasti e, più in generale, per qualsiasi verifica necessaria ad attestare la conformità con il pacchetto di norme del regolamento Europeo sulla Privacy.

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

Tutti gli attori che entrano in relazione educativa con gli studenti e le studentesse devono: mantenere sempre un elevato profilo personale e professionale, eliminando atteggiamenti inappropriati, essere guidati dal principio 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).

A tale proposito il nostro Istituto:

- ha designato la nomina di un'unità organizzativa di docenti interni ed esterni, in servizio nella nostra Istituzione Scolastica, quale incaricata del trattamento dei dati personali degli alunni necessari allo svolgimento della funzione di istruzione e assistenza scolastica. Anche i docenti esterni incaricati ufficialmente di funzioni nella scuola (esami, corsi, concorsi e attività integrative, progetti extracurricolari) entrano a pieno titolo in questa categoria;
- mette a disposizione una copia del D.L.vo 196/2003, del Regolamento UE 2016/679 e altri materiali informativi nel sito web dell'Istituto;
- ha redatto una Informativa ai sensi del D.lgs. n.196/2003 e del Regolamento Europeo 679/2016, per il trattamento dei dati personali dei dipendenti;
- ha approvato un Regolamento di Istituto per la gestione delle violazioni dei dati personali;
- si è dotato di un Regolamento recante l'identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dall'Istituto Scolastico (secondo quanto disposto dal Decreto MIUR 7 dicembre 2006, n. 305 in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali»).

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

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

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

- la pubblicazione del documento sul sito istituzionale della scuola;

- il Patto di Corresponsabilità, che deve essere sottoscritto dalle famiglie e rilasciato alle stesse all'inizio dell'anno scolastico;

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

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

CONDIVISIONE E COMUNICAZIONE DEL DOCUMENTO E-POLICY ALLA COMUNITÀ SCOLASTICA E AI GENITORI DEGLI STUDENTI E DELLE STUDENTESSE

- Le norme adottate e sottoscritte dalla scuola in materia di sicurezza e utilizzo delle tecnologie digitali saranno rese note tramite pubblicazione del presente documento sul sito web della scuola.

CONDIVISIONE E COMUNICAZIONE DELLA E-POLICY AGLI STUDENTI E ALLE STUDENTESSE

- All'inizio dell'anno, in occasione dell'illustrazione del Regolamento di Istituto agli alunni da parte dei docenti, verrà presentata la E-policy insieme ai regolamenti correlati e al Patto di corresponsabilità;
- tutti gli alunni saranno informati che la rete, l'uso di internet e di ogni dispositivo digitale saranno controllati dai docenti e utilizzati solo con la loro autorizzazione e supervisione;
- l'elenco delle regole per la sicurezza online sarà pubblicato in tutte le aule o laboratori con accesso a internet sarà data particolare attenzione nell'educazione sulla sicurezza, agli aspetti per i quali gli alunni risultano più esposti o rispetto ai quali risultano più vulnerabili, con specifico riferimento al contrasto di ogni forma di cyberbullismo.

CONDIVISIONE E COMUNICAZIONE DELLA E-POLICY AL PERSONALE SCOLASTICO

- Le norme adottate dalla scuola in materia di sicurezza dell'uso del digitale saranno discusse dagli Organi Collegiali e rese note all'intera comunità scolastica tramite pubblicazione del presente documento sul sito istituzionale;
- il personale scolastico riceverà un'adeguata informazione/formazione sull'uso sicuro e responsabile di internet, attraverso materiali resi disponibili anche sul sito istituzionale nonché mediante la partecipazione a incontri formativi organizzati dall'Istituto;
- tutto il personale è consapevole che una condotta non in linea con il codice di comportamento dei pubblici dipendenti e i propri doveri professionali è

sanzionabile.

CONDIVISIONE E COMUNICAZIONE DELLA E-POLICY AI GENITORI

- Sarà favorito un approccio collaborativo nel perseguimento della sicurezza nell'uso delle TIC e di internet in occasione di incontri scuola- famiglia, collegiali e individuali, al fine di sensibilizzare le famiglie sui temi dell'uso delle TIC;
- saranno organizzati incontri informativi per presentare e condividere la presente E-policy;
- Il documento E-policy, redatto dal Gruppo appositamente nominato e approvato dal Collegio Docenti e dal Consiglio di Istituto, sarà inserito all'interno del PTOF.

1.5 - Gestione delle infrazioni alla ePolicy

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

DISCIPLINA DEGLI ALUNNI

Le potenziali infrazioni in cui potrebbero incorrere gli alunni, relativamente alla fascia di età considerata, nell'utilizzo delle tecnologie digitali e di internet durante la didattica sono le seguenti:

- uso della Rete per giudicare, infastidire, offendere, denigrare, impedire a qualcuno di esprimersi o partecipare;
- esprimersi in modo volgare;
- invio incauto o senza permesso di foto o altri dati personali (indirizzo di casa, numero di telefono);
- condivisione online di immagini o video di compagni/e e del personale scolastico senza il loro esplicito consenso o che li ritraggono in pose offensive e denigratorie;
- condivisione di immagini intime e a sfondo sessuale invio di immagini o video volti all'esclusione di compagni/e;
- comunicazione incauta e senza permesso con sconosciuti;
- collegamenti a siti web non adeguati e non indicati dai docenti.

L'azione educativa prevista per gli alunni è rapportata alla fascia di età e al livello di

sviluppo e maturazione personale. Infatti in alcuni casi i comportamenti sanzionabili sono dovuti a uno sviluppo cognitivo, affettivo e morale incompleto o a fasi critiche transitorie, di cui gli educatori devono tenere conto per il raggiungimento di una maggiore consapevolezza e maturità da parte dell'alunno.

Pertanto sono previsti interventi graduali in base all'età e alla gravità delle violazioni:

- richiamo verbale;
- richiamo scritto con annotazione sul diario e sul registro;
- convocazione dei genitori da parte del docente;
- convocazione dei genitori da parte del Dirigente Scolastico.

Contestualmente sono previsti interventi educativi di rinforzo rispetto a comportamenti corretti e riparativi dei disagi causati, di ri-definizione delle regole sociali di convivenza, di prevenzione e gestione positiva dei conflitti, di conoscenza e gestione delle emozioni.

È inoltre importante intervenire su tutto il contesto classe con attività specifiche educative e di sensibilizzazione.

DISCIPLINA DEL PERSONALE SCOLASTICO

Le potenziali infrazioni in cui è possibile che il personale scolastico e 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 da parte degli allievi:

- utilizzo delle tecnologie e dei servizi della scuola, d'uso comune con gli alunni, non connesso alle attività di docenza o al profilo professionale, anche tramite l'installazione di software o il salvataggio di materiale non idoneo;
- utilizzo delle comunicazioni elettroniche con i genitori e gli alunni non compatibile con il ruolo professionale;
- trattamento dei dati personali e dei dati sensibili degli alunni non conforme ai principi della privacy o che non garantisca un'adeguata protezione degli stessi;
- diffusione delle password assegnate e custodia non adeguata degli strumenti e degli accessi di cui possono approfittare terzi;
- carente istruzione preventiva degli alunni sull'uso corretto e responsabile delle TIC e di internet;
- vigilanza elusa dagli alunni che può favorire un utilizzo non autorizzato delle TIC e possibili rischi connessi;
- 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 può disporre il controllo delle TIC per verificarne la conformità alle regole di sicurezza, compreso l'accesso a internet, la posta elettronica inviata/pervenuta a scuola; può disporre la cancellazione di materiali non adeguati o

non autorizzati dal sistema informatico della scuola, e se necessario ne conserva una copia per eventuali approfondimenti successivi.

Tutto il personale è tenuto a collaborare con il Dirigente Scolastico e a fornire ogni informazione utile per le valutazioni del caso e per l'avvio dei procedimenti che possono avere carattere organizzativo-gestionale, disciplinare, amministrativo, penale, a seconda del tipo e della gravità delle infrazioni commesse. Le procedure sono quelle previste dalla legge e dai contratti di lavoro.

DISCIPLINA DEI GENITORI

In considerazione dell'età degli studenti e delle studentesse e della loro dipendenza dagli adulti, anche talune condizioni e condotte dei genitori medesimi possono favorire o meno l'uso corretto e responsabile delle TIC da parte degli allievi a scuola, dove possono portare materiali e strumenti o comunicare problematiche sorte al di fuori del contesto scolastico.

Si raccomanda alle famiglie di:

- vigilare sull’uso dei dispositivi connessi alla Rete da parte dei propri figli, evitando di concedere una piena autonomia nella navigazione sul web e nell'uso di cellulare;
- evitare l’utilizzo del pc, in comune con gli adulti, che possano conservare in memoria materiali non idonei a minori;
- evitare l’utilizzo di cellulari e smartphone, in comune con gli adulti, che possano conservare in memoria indirizzi di siti o contenuti non idonei a minori.

1.6 - Integrazione dell’ePolicy con Regolamenti esistenti

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

Il nostro Istituto provvederà ad aggiornare i vari Regolamenti inserendo specifici riferimenti al presente documento.

1.7 - Monitoraggio dell'implementazione della ePolicy e suo aggiornamento

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

La prof.ssa Antonella Vedele è stata designata dal Collegio quale Referente per la revisione e/o l'aggiornamento dell'E-policy.

Il nostro piano d'azioni

Azioni da svolgere entro un'annualità scolastica

- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto agli studenti;
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto ai docenti;
- Organizzare un evento di presentazione del progetto Generazioni Connesse rivolto ai genitori.

Azioni da svolgere nei prossimi 3 anni

- Consultare i docenti dell'Istituto per la revisione e/o aggiornamento dell'E-policy.

Capitolo 2 - Formazione e curricolo

2.1. Curricolo sulle competenze digitali per gli studenti

I ragazzi usano la Rete quotidianamente, talvolta in modo più "intuitivo" ed "agile" rispetto agli adulti, ma non per questo sono dotati di maggiori "competenze digitali".

Infatti, "la competenza digitale presuppone l'interesse per le tecnologie digitali e il loro utilizzo con dimestichezza e spirito critico e responsabile per apprendere, lavorare e partecipare alla società. Essa comprende l'alfabetizzazione informatica e digitale, la comunicazione e la collaborazione, l'alfabetizzazione mediatica, la creazione di contenuti digitali (inclusa la programmazione), la sicurezza (compreso l'essere a proprio agio nel mondo digitale e possedere competenze relative alla cybersicurezza), le questioni legate alla proprietà intellettuale, la risoluzione di problemi e il pensiero critico" ("Raccomandazione del Consiglio europeo relativa alla competenze chiave per l'apprendimento permanente", C189/9, p.9).

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

L'I.C. "G.M. Gisellu" ha adottato, nel corso dell'a.s. 2017-2018, un curricolo verticale per le competenze digitali in modo tale da garantire una progressiva acquisizione delle stesse durante l'intero I° ciclo di studi, a partire dalla Scuola dell'Infanzia. (Vedi documento allegato)

Nella fase di progettazione di tale curricolo è stato fondamentale il riferimento ai seguenti documenti:

- Raccomandazione del Parlamento Europeo e del Consiglio 18.12.2006
- Indicazioni Nazionali per il Curricolo 2012
- Certificazione delle competenze C.M. 3 del 13.02.2015 e relative Linee Guida

Il curricolo è stato redatto tenendo in considerazione la definizione iniziale delle Raccomandazioni Europee, secondo la quale le competenze digitali dovranno integrare la dimensione tecnologica con quella cognitiva ed etica:

- **dimensione TECNOLOGICA**: è importante far riflettere i più giovani sul potenziale delle tecnologie digitali come strumenti per la risoluzione di problemi della vita quotidiana, onde evitare automatismi che abbiano conseguenze incerte, attraverso un'adeguata comprensione della "grammatica" dello strumento.
- **dimensione COGNITIVA**: fa riferimento alla capacità di cercare, usare e creare in modo critico le informazioni condivise in Rete, valutandone credibilità e affidabilità.
- **dimensione ETICA E SOCIALE**: la prima fa riferimento alla capacità di gestire in modo sicuro i propri dati personali e quelli altrui, e di usare le tecnologie digitali per scopi eticamente accettabili e nel rispetto degli altri. La seconda, invece, pone un po' più l'accento sulle pratiche sociali e quindi sullo sviluppo di particolari abilità socio-comunicative e partecipative per maturare una maggiore consapevolezza sui nostri doveri nei riguardi di coloro con cui comunichiamo online.

Il curricolo delle competenze digitali del nostro Istituto si basa sui seguenti TRAGUARDI DI COMPETENZE:

Al termine della Scuola dell'INFANZIA	**Al termine della Scuola PRIMARIA**	**Al termine della Scuola SECONDARIA di I grado**
• Sotto la diretta supervisione dell'insegnante utilizza le nuove tecnologie per giocare, acquisire informazioni.	• Scrive, revisiona e archivia in modo autonomo testi scritti, confeziona e invia messaggi di posta elettronica; • Con la supervisione dell'insegnane costruisce tabelle di dati e accede alla rete per ricavare informazioni, immagini, video e audio; • Conosce alcuni rischi della navigazione in rete e dell'uso delle tecnologie e adotta i comportamenti preventivi.	• Ha buone competenze digitali; • Usa con consapevolezza le tecnologie della comunicazione per ricercare e analizzare dati ed informazioni, per distinguere informazioni attendibili da quelle che necessitano di approfondimento, di controllo e di verifica e per interagire con soggetti diversi nel mondo.

L'implementazione dell'attuale curricolo per le competenze digitali sarà condotta integrando i contenuti attuali secondo le indicazioni fornite nei seguenti documenti:

- Piano Scuola Digitale (PNSD), documento di indirizzo del Ministero dell'Istruzione, dell'Università e della Ricerca;
- Sillabo sull'Educazione Civica Digitale;

- DigComp 2.1.: "Il quadro di riferimento per le competenze digitali dei cittadini";
- Raccomandazione del Consiglio europeo relativa alle competenze chiave per l'apprendimento permanente.

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

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

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

Il nostro Istituto, sin dall'anno scolastico 2013-2014, ha scelto di adottare l'uso del registro elettronico, profilando docenti e studenti sul portale ARGO.

Qualsiasi comunicazione scuola-famiglia o docente-scuola, viene caricata e trasmessa tramite questo strumento.

Attualmente l''I.C. "G.M. Gisellu" si serve della piattaforma *G-SUITE for Education* per l'attivazione delle classi virtuali, resasi indispensabile, nel corso degli ultimi anni scolastici, sia per l'erogazione delle lezioni in remoto che per uno scambio agevole di materiali tra docenti e studenti.

La presenza dell'Animatore Digitale ha permesso, anche in emergenza, la rapida risoluzione delle difficoltà connesse all'uso di entrambe le piattaforme.

Sin dalla sua designazione, coerentemente con il PNSD, l'Animatore Digitale nel nostro Istituto ha tra le sue finalità:

- FORMAZIONE INTERNA - formazione sui temi del PNSD, con l'organizzazione e/o il coordinamento di laboratori da individuare con accurata rilevazione dei bisogni.
- INNOVAZIONE - Obiettivo: promuovere e diffondere soluzioni metodologiche e tecnologiche sostenibili coerenti con l'analisi dei bisogni della nostra scuola.

In accordo con l'animatore digitale e il team, anche in futuro, verranno pertanto pianificati corsi di formazione su un uso avanzato delle TIC e delle metodologie didattiche innovative.

Tale pianificazione si avvarrà di periodiche rilevazioni delle necessità formative dei docenti.

Se necessario si potrà ricorrere anche al supporto di esperti esterni.

Verranno inoltre segnalate, con adeguata pubblicità, ulteriori opportunità ed eventi formativi in ambito digitale offerte da altre strutture presenti sul territorio e/o online.

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

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

Il nostro Istituto, nel corso dell'a.s. 2019-2020, ha proposto un corso, tenuto da personale esperto, al fine di formare i docenti sui rischi connessi ad un uso distorto della Rete da parte degli studenti e delle studentesse.

Vista l'adesione del nostro istituto al progetto SIC - "Generazioni connesse", tutti i docenti sono stati invitati a seguire i corsi proposti sulla piattaforma.

Dopo la rilevazione e l'analisi del fabbisogno formativo, si valuterà l'opportunità di proporre ulteriori corsi di formazione online e/o in presenza, aderendo a progetti esterni o promuovendo ed organizzando eventi formativi interni all'Istituto.

2.4. - Sensibilizzazione delle famiglie e

integrazioni al Patto di Corresponsabilità

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

Oltre a quelli già ricordati, tra gli obiettivi dell'Animatore Digitale, si annovera il COINVOLGIMENTO DELLA COMUNITÀ, volto a favorire la partecipazione degli studenti ad attività significative sui temi del PNSD e promuovere una cultura digitale condivisa, estesa alle famiglie.

Tra le azioni da attivare dovrà trovare necessario spazio anche la condivisione del presente documento e delle sue finalità.

In accordo con il Team e il Gruppo E-policy potranno essere proposte attività divulgative in merito ai temi di maggior rilevanza ai fini di un corretto uso e di una fruizione sicura degli strumenti informatici e della rete da parte degli studenti.

Con delibera del Collegio dei Docenti del 9.10.2020 e con delibera del Consiglio di Istituto del 14.10.2020, il nostro Istituto ha adottato il Piano per la Didattica Digitale Integrata, che contiene al suo interno, oltre informazioni generali e indicazioni di accesso alla piattaforma, anche importanti norme di comportamento alle quali è fatto obbligo attenersi.

Nel corso dell'a.s. 2020-2021, vista l'emergenza sanitaria che ha comportato una ridefinizione della didattica con l'introduzione della modalità in remoto, il "Patto di Corresponsabilità" è stato integrato con specifiche indicazioni riguardanti le norme a tutela della privacy anche nell'utilizzo degli strumenti informatici e il divieto di uso improprio dei contenuti delle lezioni e dei materiali postati ad uso didattico.

Si provvederà ad ulteriori revisioni che si rendessero necessarie, con riferimento alle Linee di indirizzo "Partecipazione dei genitori e corresponsabilità educativa" del MIUR, anche al fine di creare una maggiore collaborazione e condivisione degli interventi di formazione e di contrasto al bullismo e al cyberbullismo all'interno della comunità educante.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022)

- Effettuare un'analisi del fabbisogno formativo su un campione di studenti e studentesse in relazione alle competenze digitali.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo e l'integrazione delle TIC nella didattica.
- Effettuare un'analisi del fabbisogno formativo del corpo docente sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.

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

- Coinvolgere una rappresentanza dei genitori per individuare i temi di maggiore interesse nell'ambito dell'educazione alla cittadinanza digitale.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo e l'integrazione delle TIC nella didattica.
- Organizzare e promuovere per il corpo docente incontri formativi sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali.
- Organizzare incontri con esperti per i docenti sulle competenze digitali.
- Organizzare incontri con esperti per i genitori sull'educazione alla cittadinanza digitale.

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

3.1 - Protezione dei dati personali

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

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

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

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

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

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

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

L'Istituto Comprensivo "G.M.Gisellu" opera a ogni livello rispettando tutte le normative vigenti in merito alla tutela della privacy, come si evince dai documenti pubblicati nelle sezioni "Privacy" e "Amministrazione trasparente" collocate nella home page del sito istituzionale.

Pertanto ha cura di:

- Redigere e mantenere un registro dei trattamenti dei dati: sia per il titolare che per il responsabile dei trattamenti.
- Valutare attentamente i rischi sulla privacy relativamente ad alcune tipologie di trattamento dei dati sensibili. Le istituzioni scolastiche pubbliche e private possono trattare anche dati sensibili, come ad esempio dati relativi alle origini razziali per favorire l'integrazione degli/lle alunni/e, dati relativi alle convinzioni religiose, al fine di garantire la libertà di culto, e dati relativi alla salute per adottare misure di sostegno degli/lle alunni/e, come eventuali intolleranze alimentari o patologie che richiedono un intervento di emergenza (es. diabete, epilessia, ecc.).
- Analizzare il processo sulla raccolta/gestione del consenso verificando che la richiesta di consenso sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2). A tale proposito si rimanda alla sezione modulistica presente all'interno del notro sito web istituzionale. Verrà prestata attenzione alla formula utilizzata per chiedere il consenso: sarà comprensibile, semplice e chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali, ma devono ad esempio adeguare tutta la modulistica al Regolamento UE 2016/679 e predisporre una lettera di incarico per il trattamento dei dati al personale ATA, ai collaboratori scolastici e ai docenti.
- Adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti.

Il sito web dell'istituto comprensivo possiede già le caratteristiche necessarie per la sicurezza e la protezione dei dati trattati, in particolare:

a) immigrazione del sito da suffisso gov.it (non più validi per le istituzioni scolastiche secondo la determina n. 36 del 12 febbraio 2018) a suffisso edu.it;

b) progettazione del nuovo sito secondo i concetti di privacy by default e by design;

c) utilizzo del protocollo HTTPS (l'Hypertext Transfer Protocol Secure è un protocollo per la comunicazione su Internet che protegge l'integrità e la riservatezza dei dati

scambiati online);

d) sistema di backup (sistema che permette di salvare regolarmente i dati; ripristinare eventuali file modificati o rimossi per errore dalla rete; garantire la presenza di una copia di sicurezza di tutti i file importanti);

e) piano di disaster recovery (insieme di misure che permettono agli apparati di Information technology di superare situazioni di emergenza, ovvero di impedire che imprevisti accidentali o incidenti possano compromettere il funzionamento delle strutture).

Inoltre, verranno attuate una serie di proposte di messa in sicurezza della Rete scolastica riguardanti il cablaggio strutturato e sicuro all'interno degli edifici scolastici che si realizzerà attraverso i Fondi Strutturali Europei – Programma Operativo Nazionale "Per la scuola, competenze e ambienti per l'apprendimento" 2014-2020.

3.2 - Accesso ad Internet

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

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

comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione".

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

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

L'Istituto Comprensivo sta integrando nel sito istituzionale un Regolamento relativo all'uso delle tecnologie a scuola. In particolare suddetto Regolamento prevederà una parte dedicata all'uso di Internet in cui gli studenti si impegnano a:

- utilizzare la rete nel modo corretto;
- rispettare le consegne dei docenti;
- non scaricare materiali e software senza autorizzazione;
- non utilizzare unità removibili personali senza autorizzazione;
- tenere spento lo smartphone al di fuori delle attività didattiche che ne prevedano l'utilizzo;
- durante le attività che prevedono lo smartphone, utilizzarlo esclusivamente per svolgere le attività didattiche previste;
- segnalare immediatamente materiali inadeguati ai propri insegnanti.

I docenti si impegnano a:

- utilizzare la rete nel modo corretto;
- non utilizzare device personali se non per uso didattico;
- formare gli studenti all'uso della rete;
- dare consegne chiare e definire gli obiettivi delle attività;
- monitorare l'uso che gli studenti fanno delle tecnologie a scuola.

Per quanto concerne invece la *cybersecurity* l'Istituto si impegnerà a:

- Aggiornare periodicamente software e Sistema operativo: garantire che il sistema sia aggiornato lo protegge dalle aggressioni esterne e dalle vulnerabilità che emergono nel tempo.
- Definire la programmazione di backup periodici: cioè la copia e messa in sicurezza dei dati del sistema scolastico per prevenire la perdita degli stessi (possibilmente anche una copia offline).
- Garantire formazione adeguata allo staff, incluso il corpo docenti: la formazione

deve riguardare la gestione dei dispositivi, la conoscenza delle regole basilari sulla sicurezza.
- Testare regolarmente le possibili vulnerabilità.
- Preparare piani di azione in risposta ai problemi più seri: è importante non dover improvvisare nel momento in cui si verifica un problema serio, ma avere un protocollo di azione.
- Predisporre la disconnessione automatica dei dispositivi, dopo un certo tempo di inutilizzo: se non è previsto uno stand-by, il dispositivo resta accessibile nel caso in cui qualcuno dimentichi di spegnerlo, con il rischio potenziale di accesso da parte di persone non autorizzate.
- Impostare il browser per l'eliminazione dei cookies alla chiusura: in questo modo si evita che qualcuno possa avere accesso ad account altrui senza autorizzazione.
- Definire una policy sulle password: le password devono essere forti:
    - Richiedere password complesse con almeno 8 caratteri con numeri, maiuscole e minuscole e caratteri speciali.
    - Sensibilizzare rispetto al non uso di password facilmente identificabili (nomi dei figli, compleanni, etc.).
    - Non memorizzare le password nei dispositivi scolastici.
    - Non condividere le password con nessuno.

3.3 - Strumenti di comunicazione online

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

Per rendere maggiormente interattivo lo scambio comunicativo e al fine di valorizzare e promuovere le attività portate avanti dall'Istituto (rivolgendosi ad esempio a Istituzioni, famiglie, studenti non ancora iscritti, Associazioni), la Scuola fa riferimento al proprio sito web (https://www.istitutocomprensivodorgali.edu.it/). Inoltre, al fine di migliorare ulteriormente la comunicazione, si sta predisponendo la creazione di una pagina Facebook di Istituto.

Per quanto concerne la comunicazione interna l'Istituto utilizza il Registro

Elettronico per:

- andamento scolastico (assenze, argomenti lezioni e compiti, note disciplinari);
- risultati scolastici (voti, documenti di valutazione);
- udienze (prenotazioni colloqui individuali);
- eventi (agenda eventi);
- comunicazione varie (comunicazioni di classe, comunicazioni personali).

3.4 - Strumentazione personale

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

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

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

In riferimento al Piano Nazionale Scuola Digitale emanato dal Miur con la Legge 107 del 2015, l'IC "G.M. Gisellu" intende integrare l'utilizzo di tablet e pc personali nel lavoro nelle classi quando ben progettato e calibrato per discipline e obiettivi formativi e didattici: si pensi, a titolo di esempio, agli student response systems ossia alla possibilità degli studenti e delle studentesse di rispondere a quiz e sondaggi utilizzando direttamente il proprio smartphone come telecomando, sempre sotto la guida e il controllo dell'insegnante.

In tale ottica, verranno integrati i Regolamenti già esistenti per disciplinare l'utilizzo delle TIC all'interno della scuola (es. la dotazione di filtri), prevedere misure per prevenire diverse tipologie di rischio (non solo quelle più frequenti come il cyberbullismo) e stabilire procedure specifiche per rilevare e gestire le diverse

problematiche.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022).

- Organizzare uno o più eventi volti a consultare i docenti dell'Istituto per integrare indicazioni/regolamenti sull'uso dei dispositivi digitali personali a scuola;
- Organizzare uno o più eventi o attività volti a formare gli studenti e le studentesse dell'Istituto sul tema delle tecnologie digitali e della protezione dei dati personali;

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

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

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

4.1 - Sensibilizzazione e Prevenzione

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

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

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

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

- Nel caso della **sensibilizzazione** *si tratta di azioni che hanno come obiettivo quello di innescare e promuovere un cambiamento; l'intervento dovrebbe fornire non solo le informazioni necessarie (utili a conoscere il fenomeno), ma anche illustrare le possibili soluzioni o i comportamenti da adottare.*
- Nel caso della **prevenzione** *si tratta di un insieme di attività, azioni ed interventi attuati con il fine prioritario di promuovere le competenze digitali ed evitare l'insorgenza di rischi legati all'utilizzo del digitale e quindi ridurre i rischi per la sicurezza di bambine/i e ragazze/i.*

Il nostro Istituto intende portare avanti le seguenti **azioni di sensibilizzazione**:

- accrescere negli alunni e nelle alunne (a partire dagli ultimi anni della Scuola Primaria e per l'intero ciclo della Scuola Secondaria) la consapevolezza circa l'uso e/o l'abuso di internet, sui pericoli connessi e su come fare per evitarli;

- farli riflettere su quanto la Rete possa cambiare il loro modo di comunicare e di porsi in relazione con gli altri;
- incoraggiarli a modificare i propri comportamenti rendendoli più funzionali e sicuri;
- facilitare il coinvolgimento di soggetti esterni in modo da mettere insieme diverse idee per lavorare all'obiettivo comune.
- favorire interventi di sensibilizzazione per promuovere la conoscenza dell'e-Policy nella comunità scolastica.

Il problema della "sicurezza" è difficilmente riconducibile esclusivamente all'esistenza in sé di alcuni rischi, più o meno gravi e insidiosi, pertanto le migliori strategie di intervento sono quelle di carattere prevalentemente preventivo.

La scuola deve dunque rafforzare la sua capacità di rispondere anche a questi bisogni attraverso strumenti e misure specifiche. Allo stesso modo quando un evento problematico connesso ai rischi online coinvolge il contesto scolastico, è fondamentale per la scuola poter dare una risposta il più possibile integrata, che trovi la sua espressione di indirizzo in procedure chiare di cui deve dotarsi e che includano la collaborazione (prevedendo accordi specifici) con la rete dei servizi locali (in primis le ASL e la Polizia Postale).

Inoltre, la responsabilità dell'azione preventiva ed educativa chiama in campo diverse agenzie educative oltre alla scuola, come la famiglia, ma non solo (istituzioni, associazioni, società civile, etc.), ciascuna con un proprio compito nei confronti di bambini e bambine e di adolescenti. Tali agenzie sono chiamate a collaborare ad un progetto comune, nell'ambito di funzioni educative condivise. La necessità di supportare un uso positivo e consapevole delle TIC da parte dei più giovani, sia in un'ottica di tutela dai rischi potenziali che nella valorizzazione delle opportunità esistenti, pone la scuola e i genitori di fronte alla sfida di riconsiderare la propria identità, il proprio ruolo educativo e le proprie risorse, oltre allo stato dei rapporti reciproci per un patto educativo da rinnovare costantemente.

Pertanto l'IC "G.M. Gisellu" si propone, non solo di promuovere le competenze previste dal Curricolo digitale, ma anche le seguenti **azioni di prevenzione**:

- sensibilizzare sull'importanza di tutelare la propria privacy e quella degli altri (dati sensibili, password, foto, video) e dell'implicazioni legali in caso di trasgressione;
- far conoscere le norme etiche da rispettare quando si naviga in rete, quando si pubblica e/o si condivide un contenuto;
- riflettere su come sia possibile, dietro uno schermo, protetti dall'anonimato, infrangere con facilità tali norme, essere vittime o artefici di azioni lesive e offensive della propria e altrui persona.

4.2 - Cyberbullismo: che cos'è e come prevenirlo

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

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

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

- formazione del personale scolastico, prevedendo la partecipazione di un proprio referente per ogni autonomia scolastica;
- sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- previsione di misure di sostegno e rieducazione dei minori coinvolti;
- Integrazione dei regolamenti e del patto di corresponsabilità con specifici riferimenti a condotte di cyberbullismo e relative sanzioni disciplinari commisurate alla gravità degli atti compiuti;
- Il sistema scolastico deve prevedere azioni preventive ed educative e non solo sanzionatorie.
- **Nomina del Referente per le iniziative di prevenzione e contrasto che:**
    - Ha il compito di coordinare le iniziative di prevenzione e contrasto del cyberbullismo. A tal fine, può avvalersi della collaborazione delle Forze di polizia e delle associazioni e dei centri di aggregazione giovanile del territorio.
    - Potrà svolgere un importante compito di supporto al dirigente scolastico per la revisione/stesura di Regolamenti (Regolamento d'istituto), atti e documenti (PTOF, PdM, Rav).

Questa legge prevede la tutela dei minori per la prevenzione e il contrasto al cyberbullismo, adottando misure prevalentemente a carattere educativo/rieducativo.

Essa pone al centro il ruolo dell'Istituzione Scolastica nella prevenzione e nella

gestione del fenomeno, pertanto anche il nostro Istituto ha provveduto a individuare fra i docenti un Referente con il compito di:

- coordinare le iniziative di prevenzione e di 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;
- svolgere un importante compito di supporto al Dirigente Scolastico per la revisione/stesura di Regolamenti (Regolamento d'Istituto), atti e documenti (PTOF, PdM, Rav).

Gli atti di cyberbullismo si possono distinguere in due grandi gruppi:

1. **cyberbullismo diretto**: il bullo utilizza strumenti di messaggistica istantanea (es. sms, mms) che hanno un effetto immediato sulla vittima, poiché diretti esclusivamente a lei.
2. **cyberbullismo indiretto**: il bullo fa uso di spazi pubblici della Rete (es. social network, blog, forum) per diffondere contenuti dannosi e diffamatori per la vittima. Tali contenuti possono diventare virali e quindi più pericolosi per la vittima anche da un punto di vista psicologico.

Le **tipologie di cyberbullismo** maggiormente considerate sono:
- **Hate speech** (il fenomeno dell'incitamento all'odio, all'intolleranza verso un gruppo o una persona.
- **Dipendenza da internet e dal gioco online** (i comportamenti patologici/dipendenze).
- **Sexting** (scambio di contenuti mediali sessualmente espliciti).
- **Il grooming o adescamento online** (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).
- **Denigratio**n (diffusione di pettegolezzi, insulti, voci lesivi della dignità della persona).
- **Body shaming** (prendere in giro per l'aspetto fisico).

Salvo che il fatto costituisca reato, il Dirigente Scolastico, qualora venga a conoscenza di atti di cyberbullismo deve informare tempestivamente i genitori dei minori coinvolti (art.5).

La nostra Scuola intende portare avanti ciò che Linee prevedono ossia:

- la formazione del personale scolastico, prevedendo la partecipazione di un proprio Referente;
- lo sviluppo delle competenze digitali, tra gli obiettivi formativi prioritari (L.107/2015);
- la promozione di un ruolo attivo degli studenti (ed ex studenti) in attività di peer education;
- la previsione di misure di sostegno e rieducazione dei minori coinvolti;
- l'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.

Per intervenire efficacemente è necessario capire se si tratta effettivamente di cyberbullismo o di altra tipologia di comportamenti violenti o disfunzionali. Oltre al contesto, altri elementi utili ad effettuare questa valutazione sono le modalità in cui avvengono (alla presenza di un "pubblico"? Tra coetanei? In modo cronico e intenzionale? etc.) e l'età dei protagonisti.

Il nostro Istituto valuterà circa l'eventuale stato di disagio vissuto dalla/e persona/e minorenne/i coinvolta/e, per cui potrebbe essere necessario rivolgersi ad un servizio deputato a offrire un supporto psicologico e/o di mediazione e a centri specializzati sulla valutazione o l'intervento sul bullismo o in generale sul disagio giovanile, i comportamenti a rischio in adolescenza, etc.

Per quanto concerne la formazione, nell'a.s. 2019-2020, è stato attivato il Progetto "Identità virtuale e lotta al Cyberbullismo".

Tale progetto ha previsto degli incontri di formazione sui temi dell'identità virtuale e sulla lotta al Cyberbullismo. Gli incontri sono stati tenuti dal dottor Luca Pisano, Referente dell'Osservatorio regionale del Cyberbullismo. Sono state coinvolte tutte le classi della Scuola Secondaria con due incontri di due ore ciascuno. Il dottor Pisano ha tenuto anche un seminario di formazione diretto ai docenti e ai genitori.

Nell'a.s. 2020-2021, invece, la nostra Scuola ha partecipato a un'indagine sul Cyberbullismo (che ha visto coinvolti gli studenti, le loro famiglie e i docenti) promossa dall'Eurispes Sardegna, Istituto di Studi Politici, Economici e Sociali, in accordo con gli Assessorati Regionali alla Programmazione e Bilancio e alla Pubblica Istruzione.

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

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

Tale fenomeno, purtroppo, è sempre più diffuso ed estremamente importante

affrontarlo anche a livello educativo e scolastico con l'obiettivo di:

- fornire agli studenti gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, in particolare legati alla razza, al genere, all'orientamento sessuale, alla disabilità;
- promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network;
- favorire una presa di parola consapevole e costruttiva da parte dei giovani.

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

Lo sviluppo delle competenze digitali e l'educazione ad un uso etico e consapevole delle tecnologie assumono quindi un ruolo centrale anche per la promozione della consapevolezza di queste dinamiche in rete.

Occorre in tal senso fornire ai più giovani gli strumenti necessari per decostruire gli stereotipi su cui spesso si fondano forme di hate speech, e promuovere la partecipazione civica e l'impegno, anche attraverso i media digitali e i social network.

Si potrebbe, quindi, pensare ad attività di analisi e produzione mediale, finalizzate soprattutto a:

- 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.

In tal senso il nostro Istituto aderisce al Manifesto della comunicazione non ostile che costituisce un impegno di responsabilità condivisa e si inserisce all'interno di un Progetto sociale di sensibilizzazione contro la violenza delle parole di "Parole Ostili". Si tratta di una carta che contiene dieci principi di stile utili a favorire comportamenti rispettosi e civili, facendo della Rete un luogo accogliente e sicuro per tutti.

Inoltre, a partire dallo scorso anno scolastico, alcune classi della Scuola Secondaria di 1°grado hanno aderito al Progetto Internazionale InspirinGirls, sviluppato in Italia da Valore D, che ha l'obiettivo di lottare contro gli stereotipi di genere attraverso l'incontro in video conferenza con delle Role Models volontarie, impegnate con successo nei più diversi ruoli professionali, che offrono la loro testimonianza con la speranza che possa ampliare gli orizzonti dei/lle nostri/e ragazzi/e.

Ma già nell'a.s. 2018-2019 la nostra Scuola ha attivato degli interventi formativi finalizzati ad implementare le strategie per la riduzione degli stereotipi di genere. Il percorso è stato tenuto dalla prof.ssa Cristina Cabras del Dipartimento di Pedagogia, Psicologia, Filosofia dell'Università degli Studi di Cagliari.

Per l'anno scolastico 2020/2021 il Ministero dell'Istruzione e il Ministero della Giustizia hanno promosso il concorso di idee rivolto alle istituzioni scolastiche del territorio nazionale dal titolo "Il nuovo Codice Rosso", con lo scopo di far riflettere le studentesse e gli studenti italiani sul fenomeno della violenza di genere nella nostra società. A tale concorso ha partecipato una classe della Scuola Secondaria. Sempre nell'arco dello stesso anno, la Questura di Nuoro ha inviato dei materiali inerenti la campagna di sensibilizzazione "Questo non è amore" ideata dalla Polizia di Stato che sono stati condivisi nelle varie classi.

4.4 - Dipendenza da Internet e gioco online

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

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

Secondo uno studio del King's College di Londra più del 23% dei giovani intervistati ha una relazione disfunzionale con il proprio smartphone. Stati d'ansia provocati dalla ricerca e dall'uso compulsivo del cellulare che, nei casi più gravi, si associano a veri e propri stati depressivi.

La dipendenza da Internet, che può manifestarsi anche attraverso le ore trascorse online a giocare, rappresenta una questione importante per la comunità scolastica che deve attenzionare il fenomeno e fornire gli strumenti agli studenti e alle studentesse affinché questi siano consapevoli dei rischi che comporta l'iperconnessione.

I segnali patologici di quello che viene descritto come "un vero e proprio abuso della tecnologia", anche denominato "Internet Addiction Disorder" (I.A.D. coniato dallo psichiatra Ivan Goldberg 1996), sono:

- la tolleranza ossia quando vi è un crescente bisogno di aumentare il tempo su internet;
- l'astinenza quando, cioè, vi è l'interruzione o la riduzione dell'uso della Rete che comporta ansia, agitazione psicomotoria, fantasie, pensieri ossessivi (malessere psichico e/o fisico che si manifesta quando s'interrompe o si riduce il comportamento).

Tutto questo ha ripercussioni sulla sfera delle relazioni interpersonali che diventano

via via più povere e alle quali si preferisce il mondo virtuale, con alterazioni dell'umore e della percezione del tempo.

Spesso il trascorrere del tempo online, in termini disfunzionali, è scandito dal gioco virtuale che può anche assumere forme di Dipendenza dal gioco online (Net gaming addiction o Internet Gaming Addiction), inserito all'interno del Manuale Diagnostico Statistico dei Disturbi Mentali (DSM 5). La dipendenza si realizza quando c'è un abuso, ossia un utilizzo continuativo e sistematico della Rete al fine di giocare, impegnando la maggior parte delle giornate, con la conseguente sottrazione del tempo alle altre attività quotidiane del minore.

Il nostro Istituto si impegna a trovare delle strategie per un uso più consapevole delle tecnologie atto a favorire il "benessere digitale", cioè la capacità di creare e mantenere una relazione sana con la tecnologia.

La tecnologia infatti ha modificato gli ambienti che viviamo e ha un impatto sulla qualità della vita. Gli elementi che contribuicono al **benessere digitale** sono:

- la ricerca di equilibrio nelle relazioni anche online
- l'uso degli strumenti digitali per il raggiungimento di obiettivi personali;
- la capacità di interagire negli ambienti digitali in modo sicuro e responsabile;
- la capacità di gestire il sovraccarico informativo e le distrazioni (ad esempio, le notifiche).

Attraverso gli obiettivi e i traguardi di competenza esplicitati nel Curricolo di Educazione Civica, la nostra scuola si prefigge di contribuire alla formazione di una cittadinanza digitale che fa un uso integrativo e non sostitutivo dei dispositivi e della Rete e si pone l'obiettivo di riflettere con studenti e studentesse per fare in modo che la tecnologia sia strumento per raggiungere i propri obiettivi e non sia solo distrazione o addirittura ostacolo.

Pertanto la nostra scuola si impegna a integrare la tecnologia nella didattica, così che un suo utilizzo funzionale possa rendere più consapevoli i ragazzi e le ragazze delle proprie abitudini online. E' fondamentale far capire loro che se controlliamo la tecnologia possiamo usarne il pieno potenziale e trarne vantaggi.

Inoltre, l'IC "G.M.Gisellu" cercherà di riflettere insieme agli/lle studenti/sse sui seguenti aspetti:

- come trascorri il tempo on line?
- quando aggiunge valore alla tua vita e quando ti fa perdere tempo?
- quale atteggiamento potresti cambiare quando sei online?
- che ruolo ha e deve avere la tecnologia (internet o il gioco) nella tua vita?
- quando i videogiochi sono una risorsa?
- accedi a contenuti adeguati all'età?
- a che ora e per quanto tempo li usi?

Pertanto, ci si pone l'obiettivo di strutturare regole condivise e stipulare con loro una sorta di “patto” d’aula e, infine, proporre delle alternative metodologiche e didattiche valide che abbiano come strumento giochi virtuali d’aula (Es. adoperando la LIM) perché è importante, non demonizzare la tecnologia o il gioco, ma cercare di entrare nel mondo degli/lle studenti e delle studentesse, stabilendo chiare e semplici regole di utilizzo.

Nell'a.s. 2020-2021, la nostra scuola ha approvato un Piano per la Didattica Digitale Integrata (DDI), la metodologia innovativa di insegnamento-apprendimento rivolta a tutti gli studenti, come modalità didattica complementare che integra o, in condizioni emergenziali, sostituisce la tradizionale esperienza di scuola in presenza con l’ausilio di piattaforme digitali e delle nuove tecnologie. All'interno di tale documento sono contenute le regole condivise che gli studenti e le studentesse della nostra scuola devono rispettare. Ma già nell'a.s. 2019-2020, in seguito alla chiusura delle scuole a cusa dell'emergenza sanitaria, è stata adottata una *netiquette* condivisa, ossia un insieme di regole che dettano i parametri di educazione e buon comportamento (dal francese étiquette) sulla Rete (dall’inglese net), per un uso consapevole e rispettoso della piattaforma di Istituto.

Per l'a.s. 2021-2022, nella Scuola Secondaria di 1° grado è in fase di attivazione un Progetto Etwinning, in partenariato con una scuola francese. In tale occasione i ragazzi saranno coinvolti nella costruzione di una *netiquette* comune che li porterà a riflettere sull'importanza del rispetto delle norme quando si naviga e/o si lavora sul web insieme ad altri/e coetanei/e.

4.5 - Sexting

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

“Spesso tali immagini o video, anche se inviate ad una stretta cerchia di persone, si diffondono in modo incontrollabile e possono creare seri problemi, sia personali che legali, alla persona ritratta. L’invio di foto che ritraggono minorenni al di sotto dei 18 anni in pose sessualmente esplicite configura, infatti, il reato di distribuzione di materiale pedopornografico” (www.telefonoazzurro.it)

I contenuti sessualmente espliciti, quindi, possono diventare materiale di ricatto assumendo la forma di "revenge porn" letteralmente "vendetta porno" fenomeno quest'ultimo che consiste nella diffusione illecita di immagini o di video contenenti riferimenti sessuali diretti al fine di ricattare l'altra parte (la Legge n.69 del 19 luglio 2019, all'articolo 10 ha introdotto in Italia il reato di revenge porn, con la denominazione di diffusione illecita di immagini o di video sessualmente espliciti).

4.6 - Adescamento online

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

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

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

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

Per riconoscere un eventuale caso di adescamento online è importante prestare attenzione a piccoli gesti che possono essere indicatori importanti, come ad esempio un cambiamento improvviso nel comportamento di un minore. Per tale motivo è necessario individuare alcuni segnali che potrebbero aiutare a identificare casi di questo genere, come ad esempio:

- Il minore ha conoscenze sessuali non adeguate alla sua età?
- Venite a conoscenza di un certo video o di una foto che circola online o che il minore ha ricevuto o filmato, ma c'è imbarazzo e preoccupazione nel raccontarvi di più…
- Il minore si isola totalmente e sembra preso solo da una relazione online?
- Ci sono prese in giro e allusioni sessuali verso un/a bambino/a o ragazzo/a in

particolare?

Per prevenire casi di adescamento online è possibile accompagnare ragazze e ragazzi in un percorso di educazione (anche digitale) all'affettività e alla sessualità. A tal proposito, nell'a.s. 2019-2020, le classi seconde della Scuola Secondaria di 1°grado hanno partecipato al Progetto "Educazione alla salute e alla sessualità", proposto dal Comune di Dorgali e approvato dal Collegio dei Docenti. Gli incontri tenuti dal psicoterapeuta e sessuologo, dottor Fabrizio Quattrini, sono stati organizzati anche per i genitori e i docenti delle classi coinvolte. Purtroppo, la sospensione delle attività scolastiche in presenza, a causa dell'emergenza sanitaria, non ha reso possibile la conclusione del progetto.

In fututo il nostro Istituto si riserva di intraprendere nuove azioni per prevenire questa delicata problematica anche con l'aiuto della Polizia Postale e dei Servizi Territoriali.

4.7 - Pedopornografia

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

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

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

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

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

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

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

La nostra scuola si propone, per gli anni a venire, di promuovere azioni di sensibilizzazione rivolte a tutta la comunità scolastica.

Il nostro piano d'azioni

AZIONI (da sviluppare nell'arco dell'anno scolastico 2021/2022)

- Organizzare uno o più incontri di sensibilizzazione sui rischi online e un utilizzo sicuro e consapevole delle tecnologie digitali rivolti agli studenti/studentesse.
- Promuovere attività per studenti e studentesse dedicate all' Educazione Civica Digitale.
- Organizzare uno o più incontri per la promozione del rispetto della diversità: rispetto delle differenze di genere; di orientamento e identità sessuale; di cultura e provenienza, etc., con la partecipazione attiva degli/lle studenti/studentesse.

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

- Organizzare uno o più incontri informativi per la prevenzione dei rischi associati all'utilizzo delle tecnologie digitali, rivolti agli/lle studenti/studentesse, con il coinvolgimento di esperti.
- Organizzare uno o più incontri informativi per la prevenzione dei

rischi associati all’utilizzo delle tecnologie digitali, rivolti ai genitori e ai docenti, con il coinvolgimento di esperti.

Capitolo 5 - Segnalazione e gestione dei casi

5.1. - Cosa segnalare

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

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

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

Nelle procedure:

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

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

Nell'affrontare i casi prevediamo la **collaborazione con altre figure, enti, istituzioni e servizi presenti sul territorio** (che verranno richiamati più avanti), qualora la gravità e la sistematicità della situazione richieda interventi che esulano dalle competenze e possibilità della scuola.

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

Questo risulta importante sia per facilitare l'emersione di situazioni a rischio, e la conseguente presa in carico e gestione, sia per dare un messaggio chiaro a studenti e

studentesse, alle famiglie e a tutti coloro che vivono la scuola che la stessa è un luogo sicuro, attento al benessere di chi lo vive, in cui le problematiche non vengono ignorate ma gestite con una mobilitazione attenta di tutta la comunità.

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

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

- **Cyberbullismo**: è necessario capire se si tratta effettivamente di cyberbullismo o di altra problematica. Oltre al contesto, vanno considerate le modalità attraverso le quali il comportamento si manifesta (alla presenza di un "pubblico"? Tra coetanei? In modo ripetuto e intenzionale? C'è un danno percepito alla vittima? etc.). È necessario poi valutare l'eventuale stato di disagio vissuto dagli/lle studenti/esse coinvolti/e (e quindi valutare se rivolgersi ad un servizio deputato ad offrire un supporto psicologico e/o di mediazione).
- **Adescamento online**: se si sospetta un caso di adescamento online è opportuno, innanzitutto, fare attenzione a non cancellare eventuali prove da smartphone, tablet e computer utilizzati dalla persona minorenne e inoltre è importante non sostituirsi al bambino/a e/o adolescente, evitando, quindi, di rispondere all'adescatore al suo posto). È fondamentale valutare il benessere psicofisico dei minori e il rischio che corrono. Vi ricordiamo che l'attuale normativa prevede che la persona coinvolta in qualità di vittima o testimone in alcune tipologie di reati, tra cui il grooming, debba essere ascoltata in sede di raccolta di informazioni con l'ausilio di una persona esperta in psicologia o psichiatria infantile.
- **Sexting**: nel caso in cui immagini e/o video, anche prodotte autonomamente da persone minorenni, sfuggano al loro controllo e vengano diffuse senza il loro consenso è opportuno adottare sistemi di segnalazione con l'obiettivo primario di tutelare il minore e ottenere la rimozione del materiale, per quanto possibile, se online e il blocco della sua diffusione via dispositivi mobili.

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

Vi suggeriamo, inoltre, i seguenti servizi:

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

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

segnalare la presenza di materiale pedopornografico online.

Il nostro Istituto si attiverà tempestivamente per segnalare qualsiasi comportamento a rischio, online (ma non solo), di studenti e studentesse.

5.2. - Come segnalare: quali strumenti e a chi

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

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

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

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

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

Strumenti a disposizione di studenti/esse

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

- un indirizzo e-mail specifico per le segnalazioni;
- scatola/box per la raccolta di segnalazioni anonime da inserire in uno spazio accessibile e ben visibile della scuola;
- sportello di ascolto con professionisti;

- docente referente per le segnalazioni.

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

Nel momento in cui si è a conoscenza di situazioni di rischio:
• il docente avvisa immediatamente la Dirigente Scolastica/Responsabile di plesso/Referenti per il bullismo e il cyberbullismo;
• il docente redige una relazione sull'accaduto;
• la Dirigente Scolastica convoca, separatamente, le famiglie degli alunni coinvolti per informarle dell'accaduto e mette in atto le procedure previste dal Regolamento d'Istituto, purché i fatti non costituiscano reato.
In caso di necessità ci si può rivolgere ai servizi di supporto appositamente attivi a livello nazionale. Per segnalare contenuti inopportuni visionati sui media si può far riferimento al sito della Polizia Postale impegnata in attività a sostegno della navigazione protetta dei minori e competente a ricevere segnalazioni in merito a qualsiasi tipo di reato.

Per aiutare gli/le studenti/esse a segnalare eventuali situazioni problematiche che stanno vivendo in prima persona o di cui sono testimoni si potrebbero si prevedono alcuni strumenti di segnalazione messi a loro disposizione:

- sportello di ascolto con professionisti;
- docente referente per le segnalazioni.

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

5.3. - Gli attori sul territorio

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

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

tale percorso.

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

- **Comitato Regionale Unicef**: laddove presente, su delega della regione, svolge un ruolo di difensore dei diritti dell'infanzia.
- **Co.Re.Com. (Comitato Regionale per le Comunicazioni)**: svolge funzioni di governo e controllo del sistema delle comunicazioni sul territorio regionale, con particolare attenzione alla tutela dei minori.
- **Ufficio Scolastico Regionale**: supporta le scuole in attività di prevenzione ed anche nella segnalazione di comportamenti a rischio correlati all'uso di Internet.
- **Polizia Postale e delle Comunicazioni**: accoglie tutte le segnalazioni relative a comportamenti a rischio nell'utilizzo della Rete e che includono gli estremi del reato.
- **Aziende Sanitarie Locali**: forniscono supporto per le conseguenze a livello psicologico o psichiatrico delle situazioni problematiche vissute in Rete. In alcune regioni, come il Lazio e la Lombardia, sono attivi degli ambulatori specificatamente rivolti alle dipendenze da Internet e alle situazioni di rischio correlate.
- **Garante Regionale per l'Infanzia e l'Adolescenza e Difensore Civico**: segnalano all'Autorità Giudiziaria e ai Servizi Sociali competenti; accolgono le segnalazioni di presunti abusi e forniscono informazioni sulle modalità di tutela e di esercizio dei diritti dei minori vittime. Segnalano alle amministrazioni i casi di violazione e i fattori di rischio o di danno dovute a situazioni ambientali carenti o inadeguate.
- **Tribunale per i Minorenni**: segue tutti i procedimenti che riguardano reati, misure educative, tutela e assistenza in riferimento ai minori.

Si allega, a tale proposito, il Vademecum di Generazioni Connesse con tutti i numeri utili anche per la Regione Sardegna e le azioni da intraprendere:

http://www.generazioniconnesse.it/site/_file/documenti/Vademecum/2016/impaginato%20vademecum.pdf

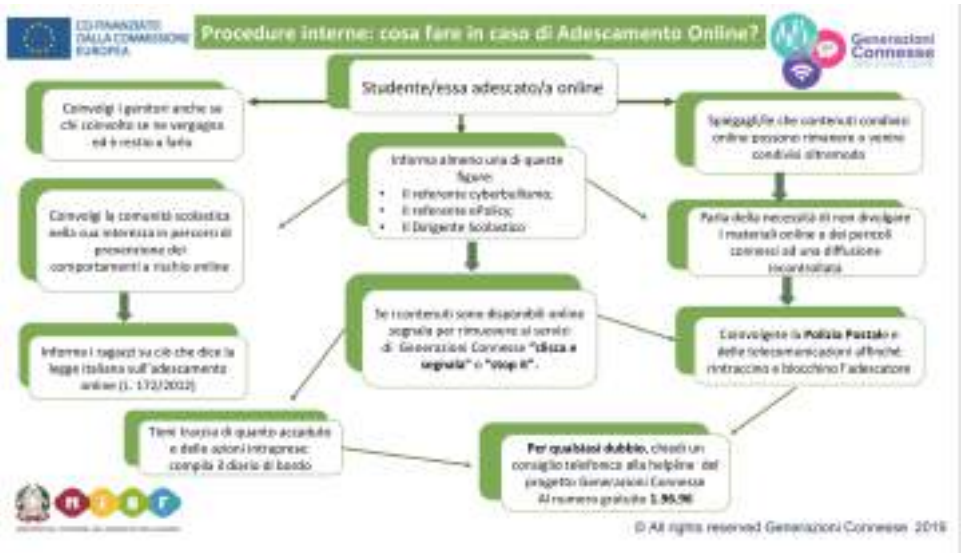
---

5.4. - Allegati con le procedure

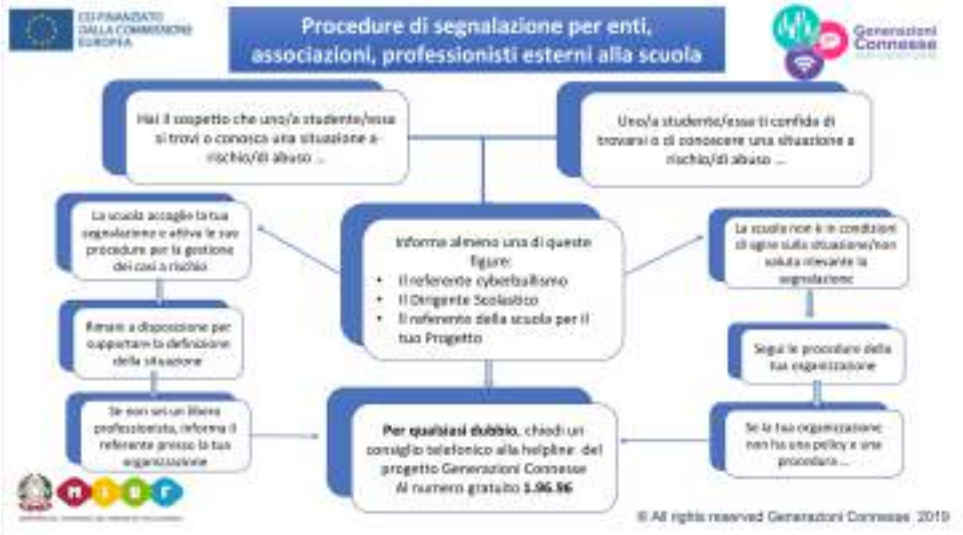
Procedure interne: cosa fare in caso di sospetto di Cyberbullismo?

Procedure interne: cosa fare in caso di sexting?

Procedure interne: cosa fare in caso di adescamento online?



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



Altri allegati

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

Procedura per la segnalazione interna in caso sospetto di cyberbullismo.

https://www.generazioniconnesse.it/_file/documenti/E-LEARNING-LEZIONI/Corso-5/1-Procedura%20di%20segnalazione%20interna%20-%20cyberbullismo.pdf

Procedura per la segnalazione interna in caso sospetto di sexting.

https://www.generazioniconnesse.it/_file/documenti/E-LEARNING-LEZIONI/Corso-5/2-Procedura%20di%20segnalazione%20interna%20-%20sexting.pdf

Procedura per la segnalazione interna in caso sospetto di adescamento online.

https://www.generazioniconnesse.it/_file/documenti/E-LEARNING-LEZIONI/Corso-5/3-Procedura%20di%20segnalazione%20interna%20-%20adescamento.pdf

Procedura per la segnalazionedi casi sospetti per enti esterni.

https://www.generazioniconnesse.it/_file/documenti/E-LEARNING-LEZIONI/Corso-5/4-Procedura%20di%20segnalazione%20enti%20esterni.pdf

Il nostro piano d'azioni

L'IC "G.M. Gisellu" si propone di realizzare una brochure informativa rivolta agli/lle studenti/sse della nostra Scuola.