ISTITUTO COMPRENSIVO
"Margherita Hack"
CASTELLALTO
VIA DEL MUNICIPIO 1, 64020 - CASTELLALTO (TE) - Telefono : 0861.296713 - Fax : 0861.320114
E-mail :teic82400b@istruzione.it - PEC : teic82400b@pec.istruzione.it - c.f. : 80003190677 - codice univoco UFQ149
Dirigente scolastico : Prof. Adriano TRENTACARLINI

E-Safety Policy

A.S. 2017/2018

Generazioni Connesse
SAFER INTERNET CENTRE

Revisione	Data	Firma Dirigente	Firma Referente
00	11/05/2018		

INDICE

1. **Introduzione**

   1.1. Scopo della Policy

   1.2. Ruoli e Responsabilità

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

   1.4. Gestione delle infrazioni alla Policy

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

2. **Formazione e Curricolo**

   2.1. Curricolo sulle competenze digitali per gli studenti

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

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

   2.4. Sensibilizzazione delle famiglie.

3. **Gestione dell'infrastruttura e della strumentazione TIC della scuola**

   3.1. Accesso ad internet

   3.2. Gestione accessi

   3.3. Sito web della scuola

   3.4. Protezione dei dati personali.

4. **Strumentazione personale**

   4.1. Per gli studenti: gestione degli strumenti personali-cellulari, tablet, ecc..

   4.2. Per i docenti: gestione degli strumenti personali-cellulari, tablet, ecc..

   4.3. Per il personale della scuola: gestione degli strumenti personali-cellulari, tablet, ecc...

5. **Prevenzione, rilevazione e gestione dei casi Prevenzione**

   5.1. Rischi

   5.2. Prevenzione

   5.3. Rilevazione

Allegato A: Scheda di segnalazione

Allegato B: Scheda per la rilevazione di violazione delle disposizioni sulla strumentazione personale

1. INTRODUZIONE

1.1.Scopo della Policy

Negli ultimi anni sempre più diffuso è l'utilizzo delle nuove tecnologie da parte di tutti. Sempre più urgente risulta pertanto essere la necessità di regolamentazione sull'uso di queste nuove tecnologie. L'istituto comprensivo "M. Hack", dopo un'attenta riflessione in merito, grazie al Piano Nazionale Scuola Digitale, alla partecipazione al progetto di Generazioni Connesse e alla sensibilità della Dirigenza e di alcuni insegnanti alle tematiche di un uso sicuro, consapevole, critico e positivo delle tecnologie digitali, vuole mettere in atto azioni mirate a sviluppare le competenze digitali dei propri alunni senza dimenticare la loro sicurezza.

Con questa ottica nasce la presente e-Safety Policy, un documento programmatico, che si prefigge di:

- ✓ Definire i principi fondamentali rispetto all'uso delle TIC in ambito scolastico.
- ✓ Indicare le norme comportamentali e le procedure per utilizzare il patrimonio TIC[1] e le risorse di questo istituto, e/o per accedere ad esse, dall'ambiente scolastico a scopo didattico/professionale da parte del personale della scuola, dei docenti e degli alunni.
- ✓ Individuare le misure per la prevenzione, per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole e/o non adeguato delle TIC.
- ✓ Assicurarsi che tutti i membri della comunità scolastica siano consapevoli che i comportamenti illeciti o pericolosi sono inaccettabili e che verranno intraprese azioni appropriate, disciplinari e/o giuridiche se necessario.

Da un'analisi dei rischi si ritiene che le principali aree di rischio per la nostra comunità scolastica, nell'uso delle TIC, sono relative all'esposizione a contenuti inappropriati, la possibilità di stringere contatti pericolosi e il rischio di cadere in comportamenti illeciti.

Per quel che riguarda i contenuti i **rischi** maggiori a cui possono essere esposti gli studenti sono:

- Esposizione a contenuti dannosi e non appropriati (es. contenuti razzisti ecc.).
- Siti web che promuovono stili di vita e comportamenti dannosi (es. siti che inneggiano al suicidio, che promuovono comportamenti alimentari scorretti, ecc.).
- Contenuti che spingono all'odio
- Pornografia

Per quel che riguarda la possibilità di stringere contatti pericolosi i rischi maggiori a cui possono essere esposti gli studenti sono:

- Grooming (adescamento online), sfruttamento sessuale
- Cyberbullismo e bullismo in tutte le forme
- Il furto di identità, comprese le password

---

1 TIC: Tecnologie dell'Informazione e della Comunicazione.

- Pedopornografia

Per quel che riguarda la possibilità di comportamenti illeciti i rischi maggiori a cui possono essere esposti gli studenti sono:

- Comportamenti aggressivi (bullismo)
- Violazione della privacy, tra cui la divulgazione di informazioni personali o di dati (foto, video, voce) senza autorizzazione dei soggetti interessati
- Reputazione digitale
- Salute e benessere:
    1. dipendenza da Internet e quantità di tempo speso online (Internet Addiction – i/le ragazzi/e che ne soffrono sono spesso inconsapevoli ma, lontani dalla Rete, manifestano presto insofferenza, irascibilità e altri sintomi di disagio)
    2. gioco d'azzardo o gambling
    3. videogiochi online in comunità mondiali (alcuni rischi associati possono essere ad esempio: contatti impropri con adulti, contenuti violenti e/o inadeguati; acquisti incontrollati, ecc.)
- Sexting
- Violazione del Copyright (poca cura o considerazione per la proprietà intellettuale e i diritti d'autore)

1.2.Ruoli e Responsabilità

Ruolo	Responsabilità
Dirigente scolastico	Deve essere adeguatamente formato sulla sicurezza e prevenzione di problematiche offline e online, in linea con le leggi di riferimento e i suggerimenti del MIUR e delle sue agenzie. Deve promuovere la cultura della sicurezza online integrandola ed inserendola nelle misure di sicurezza più generali dell'intero istituto. Ha la responsabilità di fornire sistemi per un uso sicuro delle TIC, internet, suoi strumenti ed ambienti. Ha la responsabilità della gestione dei dati e della sicurezza delle informazioni e garantisce che l'Istituto segue le pratiche migliori possibili nella gestione dei dati stessi. Deve tutelare la scuola e garantire agli utenti la sicurezza di navigazione utilizzando adeguati sistemi informatici e servizi di filtri Internet. Ha il compito di garantire a tutto il personale una formazione adeguata sulla sicurezza online per essere tutelato nell'esercizio del proprio ruolo educativo e non.

	Deve essere a conoscenza delle procedure da seguire in caso di un grave incidente di sicurezza online. Deve informare tempestivamente, qualora venga a conoscenza di atti di cyberbullismo che non si configurino come reato, i genitori del minore coinvolto (o chi ne esercita la responsabilità genitoriale o i tutori). Attiva azioni di carattere educativo nei confronti di chi ha commesso infrazioni alla policy.
Animatore Digitale	Coordinare la diffusione dell'innovazione digitale nell'ambito delle azioni previste dal POF triennale e le attività del Piano Nazionale Scuola Digitale (dal PTOF) Stimolare la formazione interna all'istituzione negli ambiti di sviluppo della "scuola digitale" e fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi; Coinvolgere la comunità scolastica (alunni, genitori e altri attori del territorio) nella partecipazione ad attività e progetti attinenti la "scuola digitale".
Referente Bullismo e Cyberbullismo	Monitorare e rilevare le problematiche emergenti relative all'utilizzo sicuro delle tecnologie digitali e di internet a scuola, nonché proporre la revisione delle politiche dell'istituzione con l'individuazione di soluzioni metodologiche e tecnologiche innovative e sostenibili da diffondere nella scuola. Organizzare eventi di prevenzione e sensibilizzazione in merito al Cyberbullismo, all'educazione all'affettività, ... anche chiedendo la collaborazione di Agenzie-Istituzioni del Territorio Collabora con il DS nella stesura e revisione della Policy e nell'integrazione dei suoi contenuti con i regolamenti d'Istituto
DSGA	Assicurare, nei limiti delle risorse finanziarie disponibili, l'intervento di tecnici per garantire che l'infrastruttura tecnica della scuola sia funzionante, sicura e non aperta a uso improprio o a dannosi attacchi esterni; Garantire il funzionamento dei diversi canali di comunicazione della scuola (sportello, circolari, sito web, ecc.) all'interno della scuola e fra la scuola e le famiglie degli alunni per la notifica di documenti e informazioni del Dirigente scolastico e dell'Animatore digitale nell'ambito dell'utilizzo delle tecnologie digitali e di internet.
Docenti	Conoscere la Policy. Educare alla sicurezza online nello svolgere il curriculo della propria disciplina. Supervisionare e guidare gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono tecnologie online.

	Garantire che gli alunni siano capaci di ricercare contenuti online in sicurezza e siano pienamente consapevoli dei problemi relativi ai contenuti elettronici. Garantire che le comunicazioni digitali dei docenti con alunni e genitori siano svolte nel rispetto del codice di comportamento professionale ed effettuate con sistemi scolastici ufficiali. Assicurare la riservatezza dei dati personali trattati ai sensi della normativa vigente. Controllare l'uso delle tecnologie digitali, dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito). Far rispettare il divieto di utilizzo di dispositivi mobili durante le ore di lezione, secondo quanto disposto nel Regolamento di Istituto. Comunicare ai genitori difficoltà, bisogni o disagi espressi dagli alunni (ovvero valutazioni sulla condotta non adeguata degli stessi) rilevati a scuola e connessi all'utilizzo delle TIC, al fine di approfondire e concordare coerenti linee di intervento di carattere educativo. Segnalare qualsiasi problema o proposta di carattere tecnico-organizzativo ovvero esigenza di carattere informativo all'Animatore digitale ai fini della ricerca di soluzioni metodologiche e tecnologiche Segnalare al Dirigente scolastico e al Referente Bullismo e Cyberbullismo qualsiasi abuso rilevato a scuola nei confronti degli alunni in relazione all'utilizzo delle tecnologie digitali o di internet, per l'adozione delle procedure previste dalle norme.
Personale ATA	Leggere, capire, firmare e aderire alla Policy di utilizzo. Contribuire alla sorveglianza nell'utilizzo da parte degli alunni di dispositivi mobili, macchine fotografiche, ecc. da parte degli alunni durante le lezioni e ogni altra attività scolastica (ove consentito).
Alunni	Essere responsabili, in relazione al proprio grado di maturità e di apprendimento, nell'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti. Non usare, senza esplicito consenso dell'insegnante, i dispositivi personali durante le attività didattiche. Avere una buona comprensione delle potenzialità offerte dalle TIC per la ricerca di contenuti e materiali ma anche della necessità di evitare il plagio e rispettare i diritti d'autore. comprendere l'importanza di adottare buone pratiche di sicurezza on-line quando si utilizzano le tecnologie digitali per non correre rischi. adottare condotte rispettose degli altri anche quando si comunica in rete. Segnalare ai propri docenti qualsiasi tipo di uso improprio dei dispositivi

	scolastici e personali di cui si venga a conoscenza.
Genitori	Sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle TIC nella didattica. Partecipare agli eventi promossi e organizzati dalla scuola. Seguire gli alunni nello studio a casa adottando i suggerimenti e le condizioni d'uso delle TIC indicate dai docenti. Concordare con i docenti linee di intervento coerenti e di carattere educativo in relazione ai problemi rilevati per un uso non responsabile o pericoloso delle tecnologie digitali o di Internet. Fissare delle regole per l'utilizzo del computer e tenere sotto controllo l'uso che i figli fanno di internet e dello smartphone in generale. Segnalare al fiduciario di plesso qualsiasi tipo di uso improprio dei dispositivi scolastici e personali di cui si venga a conoscenza da parte dell'intero personale scolastico.

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

La scuola assicurerà la promozione della condivisione degli intenti esplicitati in questo documento nel seguente modo:

1. Approvazione della Policy da parte del Consiglio d'Istituto
2. Pubblicazione nel sito web dell'Istituto
3. Invio della policy alle famiglie al momento dell'iscrizione
4. Divulgazione in occasione di incontri docenti-genitori
5. Divulgazione agli studenti al momento dell'accoglienza

1.4. Gestione delle infrazioni alla Policy

Le infrazioni alla policy possono essere rilevate da docenti o dal personale ATA nell'esercizio delle proprie funzioni oppure possono essere segnalate da alunni e genitori a docenti o personale ATA. I docenti e il personale ATA sono tenuti a dare tempestiva comunicazione di eventuali infrazioni al Dirigente Scolastico che, provvederà ad informare tempestivamente i genitori del minore coinvolto (o chi ne esercita la responsabilità genitoriale o i tutori), qualora il fatto non costituisca reato e attiverà adeguate azioni di carattere educativo. (art. 5 L. 29 maggio 2017, n. 71).

Qualora le infrazioni, invece, si configurino come vero e proprio reato il Dirigente Scolastico provvederà a tutti gli adempimenti del caso, informando gli organi di competenza.

1.5. Monitoraggio dell'implementazione della Policy e suo aggiornamento

La E-safety policy sarà riesaminata annualmente e/o quando si verificano cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola. Sarà rivista in relazione a norme di maggior valore come regolamenti o Policy emanati dal MIUR o eventuali leggi dello Stato.

2. FORMAZIONE E CURRICOLO

2.1 Curricolo sulle competenze digitali per gli studenti

Come descritto nel PTOF 2016/2019, all'interno dei curricoli di studio si inseriranno contenuti ed attività riguardanti:

1. l'educazione ai media e social network;
2. la costruzione di curricola digitali e per il digitale;
3. creazione di un curricolo di tecnologia (coding, robotica educativa, making creatività e manualità);
4. collaborazione e comunicazione in rete; dalle piattaforme digitali scolastiche alle comunità virtuali di pratica e di ricerca.

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

In conformità al PNSD, il nostro istituto ha individuato l'Animatore Digitale per il triennio 2016/2019: ins. Anna Sciamanna.

L'Istituto, all'interno del PTOF, ha individuato i seguenti interventi di **formazione**:

per l'A. S. 2016/2017:

- Pubblicizzazione e socializzazione delle finalità del PNSD con il corpo docenti.
- Formazione specifica dell'animatore digitale
- Formazione base per i docenti sull'uso degli strumenti tecnologici già presenti a scuola
- Formazione base ai docenti sull'uso delle LIM

per l'A. S. 2017/2018, il corso di formazione per i docenti "

- Formazione per i docenti all'uso degli strumenti tecnologici già presenti a scuola e all'uso di programmi di utilità e on line free per testi cooperativi, presentazioni (ppt, ecc....), video e montaggi foto (anche per i docenti della scuola dell'infanzia) o mappe e programmi di lettura da utilizzare nella didattica inclusiva

per l'A. S. 2018/2019:

- Formazione all'uso degli strumenti da utilizzare per una didattica digitale integrata
- Organizzazione e formazione per i docenti sull'utilizzo del coding nella didattica

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

In conformità con la Legge 29 maggio 2017, n. 71, il nostro Istituto ha individuato il Referente Bullismo e Cyberbullismo (2017/2019): prof. Alessandra Maccarone.

Durante l'A. S. 2017/2018 l'Istituto ha investito sulla formazione del Referente attraverso la partecipazione a due corsi di formazione, organizzati dal CTS di Nereto.

L'Istituto si impegna a:

- dare formazione regolare al personale della scuola in materia di sicurezza online e a renderlo partecipe della Policy;
- informare tutto il nuovo personale [compresi docenti in anno di prova o tirocinanti], come parte del percorso di accoglienza, con informazioni e indicazioni sulla politica di sicurezza online.

2.4 Sensibilizzazione delle famiglie

Allo scopo di mantenere viva l'attenzione delle famiglie sui tali temi, verranno valorizzate le opportunità di incontro e formazione per le famiglie sui temi oggetto della Policy, offerte dal territorio, selezionando iniziative significative promosse da Enti e/o Associazioni di comprovata affidabilità. Già da un paio di anni l'Istituto sta collaborando con l'Associazione di Genitori Ge.Co. di Castellalto per sensibilizzare le famiglie sui temi della sicurezza online, anche grazie agli incontri tenuti con la Polizia Postale.

Il coinvolgimento dell'intera Comunità scolastica è parte integrante del PTOF ed è una delle misure individuate nel Piano d'azione proposto a "Generazioni Connesse". Saranno favoriti momenti di confronto e discussione anche sulle dinamiche che potrebbero instaurarsi fra i pari con l'uso di smartphone, chat line e social network più diffusi, con particolare riferimento alla prevenzione del cyberbullismo. Si prevede la creazione di una bacheca virtuale sul sito scolastico istituzionale per la condivisione di materiali dedicati al tema del Web sicuro.

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

3.1 Accesso ad Internet e gestione accessi

L'Istituto attualmente è dotato di una rete wireless destinata all' utilizzo didattico da parte del corpo docente. La password è unica a livello di Istituto, ma la scuola sta valutando l'ipotesi di assegnare una password per ciascun utente allo scopo di monitorare meglio eventuali usi impropri e di estendere il servizio.

Ogni aula ha a disposizione una postazione con accesso ad Internet per scopi didattici e per l'accesso al Registro Elettronico. Gli alunni possono accedere alla postazione solo se preventivamente autorizzati dal docente e sotto la sua stretta supervisione.

L'Istituto è dotato di laboratori informatici 2.0 (fissi o mobili). L'accesso ai laboratori è monitorato attraverso l'utilizzo di un registro cartaceo delle presenze sul quale il docente deve apporre la

propria firma, registrare la classe, la data, l'orario di inizio e di fine e la motivazione dell'uso delle postazioni informatiche. Il registro ha lo scopo di poter risalire alle cause di eventuali inconvenienti o danneggiamenti e per comprovare l'effettivo utilizzo dell'aula. I tablet/pc dei laboratori possono essere utilizzati dagli alunni solo a scopi didattici e devono essere controllati dal docente attraverso un appropriato programma di gestione della classe virtuale.

Al termine dell'utilizzo del laboratorio sarà cura del docente lasciare il laboratorio in ordine con i pc/tablet spenti correttamente. In caso di malfunzionamento o guasto dei device bisogna darne tempestiva segnalazione al responsabile informatico o al fiduciario di plesso.

Ciascun utente connesso alla rete dovrà: rispettare il presente regolamento e la legislazione vigente succitata, tutelare la propria privacy, quella degli altri utenti adulti e degli alunni al fine di non divulgare notizie private contenute nelle documentazioni elettroniche cui ha accesso e rispettare la cosiddetta netiquette (insieme di regole, comunemente accettate e seguite da quanti utilizzano Internet e i servizi di rete, che disciplinano il comportamento di un utente nel rapportarsi agli altri utenti attraverso risorse come wiki, newsgroup, mailing list, forum, blog o e-mail).

L'Istituto si impegna a manutenere gli strumenti informatici quali antivirus e firewall al fine di impedire l'accesso a siti inappropriati. Inoltre, si impegna a mettere in atto azioni di revisione della gestione della rete wireless nell'ottica di una più completa sicurezza e tracciabilità nell'uso di internet.

3.2 Sito web della scuola

La scuola è dotata di un sito istituzionale sul quale diversi siti tematici rimandano al contenuto di interesse (Pubblicità legale, circolari, bacheca sindacale ecc).

Sul sito è possibile trovare Regolamenti, materiali didattici, pubblicizzazione di eventi, documentazione di attività curricolari ed extracurricolari svolte.

Pulsanti attivi permettono l'accesso a link di interesse tra cui il Registro Elettronico. Il sito è aggiornato quotidianamente personalmente dal Dirigente Scolastico.

3.3 Protezione dei dati personali

Si fa riferimento a quanto previsto dal Decreto legislativo 30 giugno 2003, n. 196 (Codice della Privacy) e dal Regolamento Europeo UE 2016/679 (GDPR) del 27/04/2016.

Tuttavia, si possono individuare al riguardo alcune linee guida di E-safety:

- Le fotografie o i video da pubblicare sul sito, relative a specifici eventi, che includano alunni saranno selezionati con cura e non permetteranno a singoli di essere chiaramente identificati.
- I nomi completi di alunne e alunni saranno evitati sul sito web in particolare se in associazione con le loro fotografie.
- La pubblicazione di dati personali avverrà solo nei casi previsti dalla vigente normativa.

4. STRUMENTAZIONE PERSONALE

4.1 Per gli studenti: gestione degli strumenti personali-cellulari, tablet, ecc..

Non è consentito alcun uso di strumenti elettronici personali in tutte le aree interne e di pertinenza dell'Istituto.

Solo eccezionalmente può essere consentito l'uso del cellulare in caso di urgenza per comunicazioni tra gli alunni e le famiglie, su autorizzazione e con controllo del docente.

Se uno studente viola questa policy, il dispositivo verrà confiscato e lo si terrà in un luogo sicuro in ufficio di segreteria. I dispositivi mobili saranno rilasciati solo ai genitori/tutore con delega.

I dispositivi personali possono essere utilizzati a scopi didatticisu autorizzazione e sotto il controllo del docente.

Il personale, esperti di progetto, gli studenti e i genitori o i visitatori che portano nell'Istituto i device di loro proprietà sono responsabili del proprio dispositivo e lo portano nell'Istituto a proprio rischio. Se il device si rompe, viene smarrito, viene danneggiato, vengono persi dei dati, la scuola non deve essere considerata responsabile della sicurezza di tali dispositivi/dati né deve farsi carico di eventuali risarcimenti;

La scuola si riserva il diritto di cercare contenuti in qualsiasi dispositivo mobile presente nei locali della scuola in cui vi è il ragionevole sospetto che potrebbe contenere materiale illegale o indesiderabile (es. la pornografia, la violenza o il bullismo, registrazioni di qualsiasi genere vietate, ecc...). L'ispezione avverrà alla presenza di un pubblico ufficiale.

4.2 Per i docenti: gestione degli strumenti personali-cellulari, tablet, ecc..

Durante le ore delle lezioni non è consentito l'utilizzo del cellulare, mentre è consentito l'uso di altri dispositivi elettronici personali solo a scopo didattico ed integrativo di quelli scolastici disponibili. Durante il restante orario di servizio è consentito l'utilizzo del cellulare solo per comunicazioni personali di carattere urgente mentre è permesso l'uso di altri dispositivi elettronici personali per attività funzionali all'insegnamento, ad integrazione di quelli scolastici disponibili.

4.3 Per il personale della scuola: gestione degli strumenti personali-cellulari, tablet, ecc...

Tutto il personale scolastico è autorizzato ad utilizzare device personali laddove non stia assolvendo ad un ruolo didattico, a condizione che l'utilizzo non intralci il normale svolgimento delle attività scolastiche, né distragga dal corretto svolgimento delle proprie mansioni. In tal caso la responsabilità sulla conservazione e corretta gestione degli stessi è affidata unicamente al proprietario.

5. PREVENZIONE, RILEVAZIONE E GESTIONE DEI CASI PREVENZIONE

5.1 Rischi

I rischi effettivi che si possono correre a scuola nell'utilizzo delle TIC da parte degli alunni derivano da un uso non corretto dei device personali e dei pc/tablet della scuola collegati alla rete.

Eludendo la sorveglianza degli insegnanti, attraverso i telefoni cellulari o gli smartphone, dotati di particolari applicazioni e di collegamento a internet, oltre che parlare e scrivere messaggi, gli alunni potrebbero anche scaricare e spedire foto personali o intime, proprie o di altri, video con contenuti indecenti o violenti, accedere a Internet e a siti non adatti ai minori, ascoltare musica e giocare con i videogiochi non consigliati ai minori, leggere la posta elettronica e comunicare o chattare con sconosciuti, inviare o ricevere messaggi molesti e minacciosi.

Eludendo sempre la vigilanza degli insegnanti, gli alunni potrebbero correre gli stessi rischi a scuola anche con l'utilizzo dei pc/tablet del laboratorio informatico e con un accesso non controllato a Internet.

5.2 Prevenzione

La prevenzione risulta essere sempre l'arma migliore per evitare l'insorgere di comportamenti inappropriati. Si riportano nella seguente tabella le azioni messe in atto dal nostro Istituto per prevenire i rischi di comportamenti scorretti.

RISCHIO		AZIONE
1. Utilizzo device personali durante la lezione, in classe o in altri locali di pertinenza scolastica (corridoi, bagni, spogliatoi, palestra):	a.1 per comunicare con esterni, per fotografare o girare video. a.2 per navigare in Internet ed accedere a siti sconsigliabili. a.3 per accedere ai social network e pubblicare video e foto realizzati durante le ore di lezione.	Vietare l'uso del cellulare tramite regolamento scolastico Controllare che venga rispettato il divieto Organizzare attività che promuovano l'uso corretto del cellulare e dei social networks, anche attraverso l'intervento di esperti esterni
2. Utilizzo dei dispositivi della scuola per:	2.1 per collegarsi a siti non consentiti. 2.2 scaricare materiale non consentito.	Utilizzare di sistemi di controllo per la navigazione sicura Educare a selezionare le informazioni reperibili in rete

5.3 Rilevazione

Nel caso in cui questi comportamenti scorretti si verifichino nella seguente tabella sono riportati i comportamenti da segnalare, le modalità e le azioni specifiche da intraprendere.

Che cosa segnalare	**Come segnalare: quali strumenti e a chi**	**Come gestire le segnalazioni**	**Definizione delle azioni da intraprendere a seconda della specifica del caso**
Utilizzo di device personali in orario scolastico	Si segnala al Dirigente e si contatta verbalmente la famiglia	Il docente provvede personalmente ad informare il Dirigente e la famiglia	Il device viene requisito e verrà restituito solo ai genitori o al tutore legale. Richiamo verbale nel caso

			di primo episodio. Richiamo verbale con annotazione disciplinare sul registro e sul diario personale, in caso di episodi successivi.
Uso del pc/tablet dell'Istituto per scaricare o visualizzare materiale non consentito	Si segnala al Dirigente e si contatta verbalmente la famiglia	Il docente provvede personalmente ad informare il Dirigente e la famiglia	Richiamo verbale nel caso di primo episodio. Richiamo verbale con annotazione disciplinare sul registro e sul diario personale, in caso di episodi successivi.
Utilizzo di device personali per riprendere senza autorizzazione scene di vita scolastica	Si segnala al Dirigente e per iscritto alla famiglia	Il docente provvede personalmente ad informare il Dirigente e la segreteria informerà formalmente per iscritto la famiglia.	Il device viene requisito e verrà restituito solo ai genitori o al tutore legale. Si chiede la cancellazione delle immagini ed eventualmente l'eliminazione di quelle pubblicate in internet. Richiamo verbale nel caso di primo episodio. Richiamo verbale con annotazione disciplinare sul registro e sul diario personale, in caso di episodi successivi.
Uso di device personali per compiere atti di cyberbullismo	Si segnala al Dirigente e per iscritto alla famiglia e alle agenzie di controllo	Il docente provvede personalmente ad informare il Dirigente, la segreteria informerà formalmente per iscritto la famiglia e le agenzie di controllo	Il device viene requisito e verrà restituito solo ai genitori o al tutore legale. Annotazione disciplinare sul registro. Gli atti di cyberbullismo verranno trattati dalle autorità competenti per quel che riguarda le violazioni della legislazione vigente.

Per monitorare e gestire i rischi e le rilevazioni delle infrazioni alla presente Policy si ritiene necessario avere un registro delle segnalazioni. Al presente documento sono allegate due schede:

1. Allegato A: Scheda di segnalazione
2. Allegato B: Scheda per la rilevazione di violazioni sulle norme relative all'utilizzo di device personali

Chiunque rilevi un'infrazione è tenuto alla compilazione della relativa scheda che andrà firmata e consegnata in segreteria entro 24 ore dall'evento rilevato.

L'Istituto all'inizio dell'A. S. 2018/2019 armonizzerà il presente documento con il Regolamento di Istituto attualmente in fase di rielaborazione.

SCHEDA DI SEGNALAZIONE						Allegato A E-Policy Rev. 0 (02.05.18)
ALUNNO/ALUNNI						
CLASSE		**SEZIONE**		**PLESSO**		
DOCENTE/I COINVOLTI						
DATA DELLA RILEVAZIONE		**LUOGO**				
EVENTUALI TESTIMONI (se maggiorenni)						
□ **OSSERVAZIONE DIRETTA**			□ **EVENTO RIFERITO**			
PROBLEMI EVIDENZIATI						

□ CYBERBULLISMO (rischio di molestie o maltrattamenti da coetanei)

□ ESPOSIZIONE A CONTENUTI VIOLENTI/PERICOLOSI (visita di siti pro-suicidio o pro-anoressia)

□ USO DI VIDEOGIOCHI DISEDUCATIVI

□ GIOCO D'AZZARDO ON-LINE

□ ESPOSIZIONE A CONTENUTI PORNOGRAFICI E PEDO-PORNOGRAFICI

□ GROOMING (Possibile adescamento ON-LINE)

□ SEXTING (scambio di materiale a sfondo sessuale)

□ DIPENDENZA ECCESSIVA DA INTERNET

□ ACCESSO ED UTILIZZO DI INFORMAZIONI SCORRETTE O PERICOLOSE

□ SCOPERTA ED UTILIZZO DI VIRUS IN GRADO DI INFETTARE COMPUTER

Data

_____

Firma docenti coinvolti

_____

_____

_____

Firma testimoni

_____

_____

SCHEDA PER LA RILEVAZIONE DI VIOLAZIONE DELLE DISPOSIZIONI SULLA STRUMENTAZIONE PERSONALE	Allegato B E-Policy Rev. 0 (02.05.18)

ALUNNO/ALUNNI					
CLASSE		**SEZIONE**		**PLESSO**	
DOCENTE/I COINVOLTI					
DATA DELLA VIOLAZIONE		**LUOGO**			
EVENTUALI TESTIMONI (se maggiorenni)					
DESCRIZIONE DEI FATTI					

Data

_____

Firma docenti coinvolti

_____

_____

_____

Firma testimoni

_____

_____