



ISTITUTO COMPRENSIVO STATALE DI OSTELLATO

Via Marcavallo, 35/b – 44020 Ostellato (FE) -

Tel. 0533/681191 – Fax 0533/680132

Mail: feic81400b@istruzione.it - Web: www.comprensivoostellato.gov.it

Cod. Meccanografico feic81400b - Codice fiscale: 92009650380

E-Safety Policy

Indice

Introduzione

Scopo della Policy

1) Gestione delle infrastrutture e strumentazione ICT

- Accesso ad Internet
- Account di Istituto
- Sito web della scuola
- Filtri, antivirus e sulla navigazione
- Gestione accessi (password, backup ecc.)
- Protezione dei dati personali

2) Gestione strumentazioni personali

- per gli studenti
- per il personale scolastico

3) Ruoli e responsabilità

- Dirigente scolastico
- Direttore dei Servizi Generali ed Amministrativi
- Docenti
- Studenti
- Genitori

4) Prevenzione, rilevazione e gestione dei casi

- Prevenzione
- Rilevazione e gestione dei casi
 - Che cosa segnalare
 - Come segnalare: quali strumenti e a chi

5) Formazione curricolo

- per il corpo docente
- per gli studenti
- per i genitori

Introduzione

L'approvazione da parte del Senato della Legge n. 71 del 29 maggio 2017 recante "Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo" e "Le linee di orientamento per azioni di prevenzione e di contrasto al bullismo e cyberbullismo" del 13 aprile 2015 elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con "Generazioni Connesse" e il Safer Internet Center per l'Italia - programma comunitario istituito dal Consiglio dell'Unione - inducono le istituzioni scolastiche ad adottare misure condivise affinché docenti, alunni e genitori giungano ad un uso consapevole e sicuro delle TIC¹ e, in particolare, della navigazione in rete.

E' pur vero che negli ultimi anni il nostro Istituto ha svolto una crescente azione mirata a far aumentare l'uso delle tecnologie informatiche nella didattica e nell'organizzazione generale della scuola, tanto che è ormai normale che a scuola si utilizzino LIM, portatili e tablet per connettersi al vasto mondo di Internet, sia per svolgere significative esperienze formative, sia per condurre in modo più efficiente le funzioni amministrative.

Grazie ad Internet si può facilmente fare ricerca, comunicare e documentare i propri elaborati attraverso la pubblicazione dei lavori realizzati in classe, mettendo in comune tali esperienze.

Nello stesso tempo non si può ignorare che la rete è anche una potenziale fonte di rischi, tanto più rilevanti quanto meno è diffusa una cultura relativa ai modi legittimi di usarla e alla consapevolezza delle funzioni che essa rende possibili.

Nasce perciò la necessità di limitare i pericoli connessi alla navigazione, ma al tempo stesso di utilizzare pienamente le potenzialità offerte dalle tecnologie informatiche per arricchire ed ampliare le attività didattiche, secondo quanto prevede il curriculum scolastico, l'età e la maturità degli alunni.

Scopo della Policy

Lo scopo che questa istituzione scolastica si prefigge di raggiungere mediante questa e-Safety Policy² è dunque informare e, soprattutto, formare gli utenti – docenti, alunni e genitori - affinché possano essere fortemente ridotti, se non eliminati, i rischi connessi all'uso delle TIC e della navigazione in rete.

È importante e prioritario definire all'interno dell'istituzione scolastica delle regole chiare che pongano le basi per lavorare serenamente, sicuri di aver messo in atto quanto possibile in chiave di prevenzione, ma soprattutto per usare in modo efficiente e didatticamente costruttivo le suddette tecnologie. Questa Policy perciò va intesa non come un insieme di divieti nati da generici timori, ma come stimolo ad un uso consapevole e critico delle tecnologie informatiche, con la dovuta competenza a seconda dei diversi gradi di utilizzo.

¹ TIC (o ICT - Information and Communication Technologies), acronimo per Tecnologie dell'Informazione e della comunicazione sono intese in questo documento nel più ampio senso del termine: dall'uso di software installati su Pc, all'uso di spazi di condivisione/e-learning o social, all'uso di Internet più generale, all'uso di device (dispositivi) diversi.

² Per e-Safety Policy si intende una policy di sicurezza TIC che consente di identificare le regole e le procedure per tutti gli utenti che utilizzano le risorse, il patrimonio TIC e l'accesso alla rete internet di questo istituto.

Al suo interno si andranno perciò a delineare nel tempo:

- un insieme di norme comportamentali e di procedure per utilizzare il patrimonio TIC e le risorse di questo istituto e/o per accedere ad essi anche con propri device a scopo didattico/professionale
- le misure per la prevenzione e per la rilevazione e gestione delle problematiche connesse ad un uso non consapevole/non adeguato delle tecnologie digitali, considerando la persona nella sua globalità.

La Policy, che diventerà parte integrante del Regolamento di Istituto, è un documento programmatico che impegnerà la scuola e i suoi attori anche per gli anni futuri: quanto si troverà scritto di seguito sarà realizzato gradualmente nel tempo, monitorato negli esiti rispetto alle attese prefissate, ampliato e modificato a seconda delle condizioni che man mano si manifesteranno o ci verranno suggerite dalle agenzie di riferimento, in primis Generazioni Connesse.

La nostra scuola ha già prodotto, in tal senso, nel mese di giugno 2017, un Piano d'Azione che individua il percorso e le risorse necessarie per elaborare e implementare questa Policy, individuando tre obiettivi principali:

- 1) organizzare iniziative specifiche per comunicare e far conoscere la Policy nel contesto scuola;**
- 2) promuovere la formazione di base dei docenti sull'utilizzo consapevole e sicuro di Internet e delle tecnologie digitali (soprattutto della piattaforma di Istituto messa a disposizione da Google);**
- 3) promuovere azioni di sensibilizzazione e formazione degli alunni all'utilizzo sicuro e consapevole di Internet e delle potenzialità delle tecnologie digitali anche attraverso incontri dedicati con gli esperti;**
- 4) organizzare un monitoraggio, attraverso questionari in entrata e in uscita, per verificare la ricaduta delle azioni messe in atto.**

1) Gestione delle infrastrutture e strumentazione ICT

A settembre 2017 la situazione rilevata per ciò che riguarda la strumentazione informatica presente nei 10 plessi dell'Istituto è la seguente:

PLESSO	PC FISSI	DISPOSITIVI MOBILI			POSTAZIONI CABLATE	WIFI indicare con una X la situazione del proprio plesso		
		PC PORTATILI CHROME BOOK	TABLET	ALTRO		SU TUTTO IL PLESSO	SULLA MAGGIOR PARTE DEL PLESSO	IN ALCUNI SPAZI
INFANZIA CASCINA	2	2	5			x		
LIM: 1								

INFANZIA MASSA FISCAGLIA								
INFANZIA MIGLIARINO								
INFANZIA OSTELLATO		2 notebook	1					
PRIMARIA DOGATO	15	8	38			X		
LIM: 5 su 5 classi, 1 nell'atelier								
PRIMARIA MASSA FISCAGLIA		11	19	2 netbook		X		
LIM: 6 su 8 classi								
PRIMARIA MIGLIARINO	13	8	18			X		
LIM: 4 su 8 classi								
PRIMARIA OSTELLATO	1	7 funzionanti 3 da riparare	27			X		
LIM: 7 su 7 classi								
SECONDARIA FISCAGLIA	10	14	19		13	X		
LIM: 9 su 9 classi + 1 in aula musica								
SECONDARIA OSTELLATO	11	6	18		10	x		
LIM: 5 su 6 classi								

- Accesso ad Internet

A giugno 2017 la situazione per ciò che riguarda la tipologia di connessione ad Internet presente nei 10 plessi dell'Istituto è la seguente³:

PLESSO	TIPOLOGIA DI CONNESSIONE AD INTERNET	GESTORE	CANONE A CARICO DI
INFANZIA CASCINA	Connettività fibra ottica (Secondaria standard)	Lepida S.P.A. Delta Web	

³ Siamo in attesa del completamento della tabella da parte delle amministrazioni comunali

INFANZIA MASSA FISCAGLIA	Connettività fibra ottica (Secondaria standard)	Lepida S.P.A. Delta Web	Amministrazione comunale
INFANZIA MIGLIARINO	Connettività fibra ottica (Secondaria standard)	Lepida S.P.A. Delta Web	Amministrazione comunale
INFANZIA OSTELLATO			Amministrazione comunale
PRIMARIA DOGATO	Connettività accesso dati SYN 4 Banda 6,5 MB	Telecom Italia Spa	Amministrazione comunale
PRIMARIA MASSA FISCAGLIA	Connettività fibra ottica (Secondaria standard)	Lepida S.P.A. Delta Web	Amministrazione comunale
PRIMARIA MIGLIARINO	Connettività fibra ottica (Secondaria standard)	Lepida S.P.A. Delta Web	Amministrazione comunale
PRIMARIA OSTELLATO	Connettività con tecnologia radio Banda 8 MB	Delta Web Spa	Amministrazione comunale
SECONDARIA FISCAGLIA	Connettività fibra ottica (Secondaria standard)	Lepida S.P.A. Delta Web	Amministrazione comunale
SECONDARIA OSTELLATO	Connettività con tecnologia radio Banda 8 MB	Delta Web Spa	Amministrazione comunale

- Account di Istituto

All'inizio di ogni anno scolastico l'Amministratore di Sistema consegna al coordinatore di plesso la pw per l'utilizzo dei servizi di rete del plesso - accesso ad Internet - e l'aggiornamento degli account degli studenti e degli insegnanti. Sarà cura del coordinatore conservare e non condividere la pw di accesso alla rete, inserirla personalmente nei dispositivi in possesso del plesso che accedono ad Internet ed eventualmente inserirla nei dispositivi personali degli insegnanti che lo richiedessero. A questo proposito il coordinatore comunicherà al Dirigente i nomi degli insegnanti che hanno

chiesto di accedere alla rete tramite la connessione della scuola utilizzando un proprio devices indicando la tipologia del dispositivo medesimo.

Questo tipo di controllo si rende necessario in quanto ad oggi nessun plesso è dotato di un sistema di accesso tramite l'identificazione dell'utente.

Per quel che riguarda la sede (scuola primaria e secondaria) e il plesso di scuola primaria di Dogato, sede dell'atelier di Istituto, la pw di accesso alla rete, per motivi di servizio, sarà nota al Dirigente ed allo staff per consentirne l'utilizzo con dispositivi personali nel corso degli incontri di servizio programmati. Per la scuola di Dogato si deve prevedere che l'accesso alla rete possa avvenire anche da devices di proprietà di coloro che chiederanno di utilizzare gli spazi dell'atelier, pertanto la pw sarà resa nota al responsabile esterno che richiederà l'uso dei locali.

Poiché l'Istituto si avvale di un dominio **@ostellato.istruzioneer.it** gli account in possesso di tutti gli utenti sono di proprietà dell'Istituto che come tale fornisce un servizio. Le famiglie riceveranno tramite una comunicazione scritta i riferimenti (indirizzo di posta elettronica e pw) e le relative norme di utilizzo che per accettazione sottoscriveranno.

Gli utenti del dominio di istituto hanno abilitati servizi specifici a seconda della categoria a cui appartengono. In particolare:

1. gli account degli insegnanti possono accedere a tutti i servizi abilitati della G Suite, in particolare possono utilizzare il servizio di mail anche per indirizzi diversi da quello di istituto;
2. gli studenti hanno abilitati alcuni servizi e non possono ricevere o inviare mail ad indirizzi diversi da quello di istituto. Gli studenti per l'utilizzo del loro account devono utilizzare la pw che è stata loro consegnata in modo tale da consentire anche ai docenti di entrare nell'account per funzioni di controllo.

Per ciò che riguarda i servizi con una funzione "social" sono abilitati all'apertura di un blog solo gli account di servizio. Nel caso un docente o un gruppo di docenti manifestassero l'esigenza di aprire un blog dovranno farne richiesta al Dirigente e all'Animatore Digitale che provvederà ad aprire il blog e a comunicare le modalità di accesso. E' implicito che colui e/o coloro che effettueranno la domanda saranno responsabili dei post e del materiale pubblicato.

Gli insegnanti sono tenuti ad utilizzare l'accesso alla rete "solo ed esclusivamente" per finalità professionali:

- condividere documenti con alunni e/o colleghi;
- effettuare ricerche in rete a scopo didattico
- controllare la posta di plesso;
- consultare il sito web dell'Istituto;
- compilare il registro elettronico;
- inviare mail per finalità istituzionali e connesse all'attività lavorativa.

Ogni utente è responsabile personalmente dell'account e dell'uso che ne viene fatto. Nel rispetto del regolamento d'Istituto, il Dirigente scolastico e l'Amministratore di Sistema si riservano la facoltà di monitorare ed eventualmente di eseguire controlli e verifiche sul corretto utilizzo dei servizi Internet e posta elettronica.

In caso di illeciti, si procederà all'invio di avvisi individuali e si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro. Se questo non dovesse essere sufficiente, sarà attivato un procedimento disciplinare nelle forme e con le modalità di cui al D.lgs. n. 165 del 2001 articoli 55 bis e seguenti.

- Sito web della scuola.

L'Istituto dispone di un proprio sito web al seguente indirizzo:



<http://www.comprensivoostellato.gov.it>





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

Il web master, esperto esterno incaricato dal Dirigente scolastico, si occupa della gestione del sito, mentre un incaricato fra il personale docente ha il compito di inserire nel sito web i contenuti che egli stesso predispone su indicazione del Dirigente o che gli vengono trasmessi dai singoli plessi. Anche l'Animatore Digitale è autorizzato ad inserire contenuti sul sito. Il personale di segreteria pubblica autonomamente i contenuti di pertinenza utilizzando il software proprietario del registro elettronico di cui si è dotata la scuola.

Si sottolinea che i docenti sono direttamente responsabili dei prodotti che inviano per la pubblicazione sul sito web dell'istituto e pertanto devono prestare la massima attenzione nel riutilizzare i contenuti reperiti in rete (immagini, video, file audio, file di testo...)

Per non incorrere nella violazione previste dalla normativa sui diritti d'autore si dispone che i materiali siano rispettosi delle regole vigenti per le licenze Creative Commons di seguito riportate:

Simboli	Sigla	Descrizione
	CC BY	Permette di distribuire, modificare, creare opere derivate dall'originale, anche a scopi commerciali, a condizione che venga: riconosciuta una menzione di paternità adeguata, fornito un link alla licenza e indicato se sono state effettuate delle modifiche. ^[5]
	CC BY-SA	Permette di distribuire, modificare, creare opere derivate dall'originale, anche a scopi commerciali, a condizione che venga: riconosciuta una menzione di paternità adeguata, fornito un link alla licenza e indicato se sono state effettuate delle modifiche; e che alla nuova opera venga attribuita la stessa licenza dell'originale (quindi ad ogni opera derivata verrà consentito l'uso commerciale). ^[6] Questa licenza, per certi versi, può essere ricondotta alle licenze "copyleft" del software libero e open source.

	CC BY-ND	<p>Permette di distribuire l'opera originale senza alcuna modifica, anche a scopi commerciali, a condizione che venga riconosciuta una menzione di paternità adeguata e venga fornito un link alla licenza.</p> <p>Quindi non consente la distribuzione di opere modificate, remixate o basate sull'opera licenziata con questa licenza.^[7]</p>
	CC BY-NC	<p>Permette di distribuire, modificare, creare opere derivate dall'originale, ma non a scopi commerciali, a condizione che venga: riconosciuta una menzione di paternità adeguata, fornito un link alla licenza e indicato se sono state effettuate delle modifiche.</p> <p>Chi modifica l'opera originale non è tenuto ad utilizzare le stesse licenze per le opere derivate.^[8]</p>
	CC BY-NC-SA	<p>Permette di distribuire, modificare, creare opere derivate dall'originale, ma non a scopi commerciali, a condizione che venga: riconosciuta una menzione di paternità adeguata, fornito un link alla licenza e indicato se sono state effettuate delle modifiche; e che alla nuova opera venga attribuita la stessa licenza dell'originale (quindi ad ogni opera derivata non verrà consentito l'uso commerciale).^[9]</p>
	CC BY-NC-ND	<p>Questa licenza è la più restrittiva: consente soltanto di scaricare e condividere i lavori originali a condizione che non vengano modificati né utilizzati a scopi commerciali, sempre attribuendo la paternità dell'opera all'autore.^[10]</p>

- Filtri, antivirus e sulla navigazione

Ad oggi l'accesso ad internet in tutti i plessi dell'Istituto non è sottoposto a filtri, non disponendo di connessioni sulle quali poter procedere con accessi personali tramite un identificativo la navigazione di tutto il personale scolastico - dirigente, amministrativi, personale ATA, docenti, studenti - non è soggetta ad alcuna restrizione. Pertanto sul versante prettamente didattico è fatto obbligo al personale docente di prestare la massima attenzione nell'utilizzo didattico della rete da parte degli alunni. Dal canto loro gli studenti potranno accedere alla rete solo ed esclusivamente col permesso del docente che ne controlla la navigazione.

Tenuto conto della effettiva situazione dell'Istituto si cercherà di sensibilizzare tutta la comunità scolastica sulle regole basilari sulla navigazione sicura, anche attraverso l'attuazione di incontri specifici rivolti a docenti, studenti e famiglie, sull'opportunità di utilizzare semplici programmi di ottimizzazione dei PC e di mantenere aggiornati gli antivirus installati sia sulle postazioni fisse che dispositivi mobili; inoltre ci si educherà ad utilizzare il più possibile il Cloud, per evitare l'utilizzo di dispositivi di archiviazione esterna di proprietà che comunque vanno controllati prima di essere utilizzati sui dispositivi della scuola onde evitare danni causati da virus e malware.

- **Gestione accessi (password, backup ecc.)**

La scuola adotterà tutte le necessarie precauzioni per evitare l'accesso a siti non adatti all'interno della scuola. I docenti possono accedere alla propria sezione del registro elettronico con credenziali personali. Anche a genitori e alunni sono state fornite credenziali personali di accesso al registro elettronico, il cui backup viene eseguito dal sistema periodicamente e i dati preservati in cloud. I dati personali vengono trattati nel rispetto della normativa sulla privacy.

- **Protezione dei dati personali**

In un momento in cui il confine tra pubblico e privato sembra essere costantemente messo in discussione, è necessario imparare a gestire i propri dati sensibili e a tutelarli, anche alla luce delle strategie di web marketing e profilatura dell'utente. Per questo motivo il personale scolastico è "incaricato del trattamento" dei dati personali (degli alunni, dei genitori, ecc.), nei limiti delle operazioni di trattamento e delle categorie di dati necessarie ai fini dello svolgimento della propria funzione e nello specifico della docenza (istruzione e formazione). Le nuove tecnologie della comunicazione, dai blog ai wiki, ai social network, consentono di condividere pubblicamente le informazioni personali e ciò solleva nuove e pressanti questioni per la tutela della privacy e dei dati sensibili. Molti giovani condividono con disinvoltura informazioni personali su siti e social network, accessibili al largo pubblico come Facebook. Oltre al problema dell'esposizione dei dati sensibili, vi è quello del tracciamento delle informazioni personali dell'utente per usi commerciali. Le strategie di web marketing si basano infatti sulla possibilità di conoscere e delineare un profilo preciso dell'utente attraverso il tracciamento delle sue azioni e di utilizzare gli utenti stessi come generatori e promotori di contenuti pubblicitari. Per un uso consapevole e sicuro dei nuovi media, in particolare Internet, occorre allora rendere le persone capaci di gestire in modo selettivo e pertinente le informazioni condivise elettronicamente. Per questo motivo ai genitori viene fornita una informativa sul trattamento dei dati personali ai sensi dell'Art. 13 del D. Lgs. 30 giugno 2003, n. 196, e richiesta di autorizzazione all'utilizzo dei dati personali degli alunni eccedenti i trattamenti istituzionali obbligatori, come ad esempio l'utilizzo di fotografie, video o altri materiali audiovisivi contenenti l'immagine, il nome e la voce del proprio figlio/a, all'interno di attività educative e didattiche per scopi documentativi, formativi e informativi, durante gli anni di frequenza della scuola. A tale proposito si evidenzia che le immagini e le riprese audio-video realizzate dalla scuola, nonché gli elaborati prodotti dagli studenti durante le attività scolastiche, potranno essere utilizzati esclusivamente per documentare e divulgare le attività della scuola tramite il sito internet di Istituto, pubblicazioni, mostre, corsi di formazione, seminari, convegni e altre iniziative promosse dall'Istituto anche in collaborazione con altri enti pubblici.

L'autorizzazione non consente l'uso dell'immagine in contesti che pregiudichino la propria dignità personale ed il decoro e comunque per uso e/o fini diversi da quelli sopra indicati.

2) Gestione strumentazioni personali

- **per gli studenti**

A scuola è attualmente vietato l'uso per scopo personale di tutti gli strumenti informatici di proprietà dello studente e, in particolare, dei telefoni cellulari. All'entrata in classe il docente della

prima ora provvederà al loro ritiro, riponendoli in un apposito contenitore che sarà chiuso a chiave in un armadio o in un cassetto predisposto allo scopo. Nel caso in cui debbano comunicare con la famiglia durante l'orario scolastico, alunne e alunni possono usare la linea fissa della scuola; allo stesso modo le famiglie devono chiamare la scuola se hanno assoluta necessità di parlare con i propri figli. Si raccomanda di ridurre tali comunicazioni a casi di inderogabile necessità e urgenza.

L'eventuale utilizzo di strumenti informatici di proprietà dello studente durante una specifica attività didattica è consentito (previo consenso firmato del genitore e senza responsabilità della scuola) unicamente su autorizzazione e indicazione del docente e con esclusiva finalità didattica. Le modalità di utilizzo concordate prevedono comunque la vigilanza costante del docente stesso. È vietato usare dispositivi di registrazione audio, video o fotografica per registrare media o fare foto senza il permesso dell'insegnante e senza il consenso della persona che viene registrata o fotografata. Audio e video realizzati a scuola possono essere pubblicati esclusivamente dai docenti, dietro autorizzazione dei genitori, per fini didattici. Previa consultazione con il Consiglio di Classe, si concorderanno le modalità di impiego di strumenti compensativi quali tablet e computer portatili e le modalità di custodia degli stessi.

Si richiama l'attenzione degli alunni, dei docenti e delle famiglie sulle possibili conseguenze di eventuali riprese audio/video o fotografie effettuate all'interno degli ambienti scolastici, al di fuori dei casi consentiti, e successivamente diffuse con l'intento di ridicolizzare compagni o insegnanti o addirittura allo scopo di intraprendere azioni che sono spesso definite con il termine di cyberbullismo. Tali azioni possono configurare, nei casi più gravi, gli estremi di veri e propri reati.

- per il personale scolastico

Il personale scolastico utilizzerà, quando ciò è possibile, l'impiego della strumentazione fornita dalla scuola rispetto a quella personale (portatili, pc fissi, ...); le infrastrutture e gli apparati della scuola non vanno utilizzati per scopi personali. Telefoni cellulari, tablet, fotocamere e altri strumenti di registrazione audio/video non devono essere impiegati durante le lezioni scolastiche se non all'interno di attività didattiche espressamente programmate. La password di accesso alla rete wireless va custodita con cura e per nessuna ragione deve essere divulgata a chi non ha titolo per utilizzarla (studenti, genitori, operatori esterni). Qualora si utilizzino a scuola dispositivi di archiviazione esterna di proprietà personale (chiavette usb, dischi fissi portatili) è bene controllare preventivamente che essi siano esenti da virus per evitare di danneggiare le attrezzature comuni.

3) Ruoli e responsabilità

Nell'ambito di questa policy sono individuati i seguenti ruoli e le principali responsabilità correlate:

- Dirigente scolastico:

- garantire la tutela degli aspetti legali riguardanti la privacy e la tutela dell'immagine di tutti i membri della comunità scolastica;
- garantire 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;

- garantire l'esistenza di un sistema che consenta il monitoraggio e il controllo interno della sicurezza on line;
- comprendere e seguire le procedure previste dalle norme in caso di reclami o attribuzione di responsabilità al personale scolastico in relazione a incidenti occorsi agli alunni nell'utilizzo delle TIC a scuola.

- Animatore digitale come da PNSD:

- stimolare la formazione interna alla scuola negli ambiti del PNSD, attraverso l'organizzazione di laboratori formativi, favorendo l'animazione e la partecipazione di tutta la comunità scolastica alle attività formative, come ad esempio quelle organizzate attraverso gli snodi formativi;
- 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;
- fornire consulenza e informazioni al personale in relazione ai rischi on-line e alle misure di prevenzione e gestione degli stessi;
- favorire la partecipazione di tutti nell'organizzazione di workshop e altre attività, anche strutturate, sui temi del PNSD, anche attraverso momenti formativi aperti alle famiglie e ad altri attori del territorio, per la realizzazione di una cultura digitale condivisa;
- individuare e creare soluzioni metodologiche e tecnologiche sostenibili ed innovative da diffondere all'interno degli ambienti della scuola (es. uso di particolari strumenti per la didattica di cui la scuola si è dotata; adozione di metodologie comuni; informazione su innovazioni esistenti in altre scuole; laboratorio di coding per tutti gli studenti), coerenti con l'analisi dei fabbisogni della scuola stessa, anche in sinergia con attività di assistenza tecnica condotta da altre figure.

- Direttore dei Servizi Generali e Amministrativi:

- assicurare, 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;
- facilitare la trasmissione di comunicazioni relative alle tecnologie digitali tra le varie componenti della scuola (Dirigente scolastico, Animatore digitale, docenti e famiglie degli alunni);
- curare la registrazione dei disservizi e delle problematiche relative alla rete e all'uso del digitale segnalate dai docenti, provvedendo all'intervento del personale tecnico di assistenza.

- Personale ATA:

- avere adeguata consapevolezza circa le questioni di sicurezza informatica e la politica dell'Istituto e relative buone pratiche;
- aver letto, compreso e sottoscritto la presente policy;
- segnalare qualsiasi abuso, anche sospetto, al Dirigente Scolastico o all'Animatore Digitale per le opportune indagini/azioni/sanzioni;
- mantenere tutte le comunicazioni digitali con alunne/alunni e genitori/tutori a livello professionale e realizzarle esclusivamente con sistemi ufficiali scolastici.

- Docenti:

- formarsi e aggiornarsi sulle problematiche attinenti alla sicurezza nell'utilizzo delle tecnologie digitali e di Internet e sulla politica di sicurezza adottata dalla scuola, rispettandone il regolamento;
- sviluppare le competenze digitali degli alunni e fare così in modo che conoscano e seguano le norme di sicurezza nell'utilizzo del web e utilizzino correttamente le tecnologie digitali sia a scuola sia nelle attività didattiche extracurricolari condividendo con essi la *netiquette*, ovvero l'insieme di regole di comportamento volte a favorire il reciproco rispetto tra gli utenti;
- assicurare che gli alunni abbiano una buona comprensione delle opportunità di ricerca offerte dalle tecnologie digitali e dalla rete, ma anche della necessità di evitare il plagio e di rispettare la normativa sul diritto d'autore;
- 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;
- segnalare prontamente alle famiglie eventuali problematiche emerse in classe nell'utilizzo del digitale e stabilire comuni linee di intervento educativo per affrontarle;
- 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 innovative da diffondere nella scuola e di un aggiornamento della politica adottata in materia di prevenzione e gestione dei rischi nell'uso delle TIC;
- segnalare al Dirigente scolastico e ai suoi collaboratori eventuali episodi di violazione delle norme di comportamento stabilite dalla scuola, avviando le procedure previste in caso di violazioni.

- Studenti:

- essere responsabili, in relazione al proprio grado di maturità e di apprendimento, per l'utilizzo dei sistemi delle tecnologie digitali in conformità con quanto richiesto dai docenti;

- 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 (*netiquette*);
- esprimere domande o difficoltà o bisogno di aiuto nell'utilizzo delle tecnologie didattiche o di internet ai docenti e ai genitori.

- Genitori:

- aver letto, compreso e sottoscritto la presente policy;
- sostenere la linea di condotta della scuola adottata nei confronti dell'utilizzo delle tecnologie dell'Informazione e delle Comunicazioni nella didattica;
- contribuire, in sinergia con il personale scolastico, alla sensibilizzazione dei propri figli sul tema della sicurezza in rete;
- incoraggiare l'impiego delle TIC da parte degli alunni nello svolgimento dei compiti a casa, controllando che tale impiego avvenga nel rispetto delle norme di sicurezza;
- 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;
- agire in modo concorde con la scuola per la prevenzione dei rischi e l'attuazione delle procedure previste in caso di violazione delle regole stabilite.

4) Prevenzione, rilevazione e gestione dei casi

- Prevenzione

I rischi nei quali è possibile che gli alunni incorrano, nell'utilizzo delle TIC, possono derivare da un uso inappropriato delle strumentazioni personali o di quelle della scuola.

Per prevenirli, contrastarli ed affrontarli, è necessario l'impegno di tutti: comunità scolastica e genitori.

Occorre sviluppare sia le loro competenze digitali sia quelle emotivo-relazionali, promuovendo una cultura dell'inclusione, del rispetto di sé e dell'altro.

È necessario accompagnare gli alunni nella navigazione in rete, creare occasioni di confronto tra loro, con gli insegnanti o con esperti.

Oltre a ciò, è indispensabile che i ragazzi sappiano, nel caso in cui si trovino in una situazione di pericolo, come e a chi chiedere aiuto.

RISCHI	AZIONI DI PREVENZIONE
VIOLAZIONE DELLA PRIVACY	La scuola promuove lo sviluppo della capacità di gestire i dati personali in maniera consapevole, a partire dalla conoscenza di un uso sicuro delle credenziali di accesso alla rete. È necessario creare occasioni in cui genitori, alunni e docenti possano

	confrontarsi con esperti su come utilizzare le impostazioni di privacy dei loro dispositivi e dei social network che frequentano.
CONTENUTI NON ADATTI	I dispositivi e la rete della scuola devono essere dotati di software di protezione che impediscano l'accesso a siti con contenuti non adatti agli alunni. È fondamentale, a tal proposito, che la scuola e la famiglia educino i ragazzi affinché essi siano in grado di discriminare ed evitare siti sconsigliati ed eventualmente siano anche capaci di segnalarne i contenuti inopportuni.
GROOMING	La scuola, insieme alla famiglia, deve aiutare i ragazzi a proteggersi e tutelarsi, scegliendo con cura chi frequentare online. Gli insegnanti devono spiegare agli alunni che qualsiasi contenuto pubblicato o condiviso può potenzialmente essere visto e diffuso da chiunque. Essi devono imparare a chiedere aiuto per loro e per gli altri e ad informare sempre gli adulti di cui si fidano di eventuali richieste di incontri ricevute da contatti conosciuti online.
CYBERBULLISMO	Per prevenire e affrontare il cyberbullismo, i docenti intervengono sul gruppo classe, ad esempio con percorsi volti alla gestione positiva del conflitto. Tutto ciò per evitare il diffondersi di comportamenti offensivi e persecutori ai danni di altri, ad esempio attraverso la divulgazione di messaggi o la pubblicazione di foto o filmati che ritraggono prepotenze o in cui compagni o compagne sono diffamati.
SEXTING	La scuola accompagna i ragazzi nella conoscenza della loro corporeità e affettività proponendo percorsi e progetti che promuovano il senso di fiducia, l'autostima e l'instaurarsi di relazioni autentiche e rispettose. Essi devono essere resi consapevoli dei rischi e delle possibili conseguenze legali legate alla produzione e diffusione di messaggi e/o immagini a sfondo sessuale o della creazione e condivisione di immagini di nudo o seminudo in rete.

- Rilevazione e gestione dei casi

❑ Che cosa segnalare

L'utilizzo incauto o scorretto degli strumenti digitali afferisce ai seguenti casi:

1. contenuti relativi alla privacy: foto personali, indirizzo di casa, numero di telefono, informazioni private proprie o di altri, foto o video pubblicati contro la propria volontà.
2. contenuti violenti o aggressivi: messaggi minacciosi, commenti offensivi, foto o video imbarazzanti, contenuti con messaggi a sfondo razzista, immagini o video umilianti, insulti.
3. contenuti a sfondo sessuale: messaggi molesti, conversazioni che ravvisano una relazione intima, foto o video personali con nudità o abbigliamento succinto, immagini pornografiche, foto e video in cui persone di minore età sono coinvolte o assistono ad attività sessuali.

❑ **Come segnalare: quali strumenti e a chi**

Gli insegnanti devono conservare le prove della condotta imprudente, scorretta o dell'abuso rilevati sulle strumentazioni della scuola.

Conservarle è molto importante per far conoscere l'accaduto ai genitori degli alunni, al Dirigente scolastico, alla Polizia Postale o all'autorità giudiziaria competente.

Qualora non si disponga di prove tangibili, ma solo della testimonianza dell'alunno, anche se fosse riferita a fatti accaduti al di fuori della scuola, le informazioni raccolte sono comunque da segnalare al Dirigente Scolastico e ai genitori, per valutare il da farsi.

Le segnalazioni coinvolgeranno tutte le persone o autorità menzionate e l'uso degli strumenti di seguito citati:

1. annotazione del comportamento sul Registro di classe e comunicazione scritta ai genitori.
2. Convocazione scritta da parte dei docenti e colloquio con i genitori degli alunni.
3. Relazione scritta al Dirigente scolastico.
4. Denuncia agli organi di polizia territorialmente competenti o all'autorità giudiziaria.

5) Formazione curricolo

L'Istituto Comprensivo per evitare che l'adozione di questa policy rappresenti esclusivamente un atto formale, si impegna a farla diventare una base di partenza per una serie di azioni e iniziative in itinere. Si partirà, innanzitutto, dalla sua pubblicazione sul sito della scuola www.comprensivoostellato.gov.it. Si propongono inoltre le seguenti azioni:

- per il corpo docente:

- discutere collegialmente sui contenuti, sulle pratiche indicate e su come inserire nel curricolo le tematiche di interesse della policy;
- stabilire momenti di confronto, su base annuale, circa la necessità di apportare modifiche e miglioramenti alla policy vigente;
- elaborare protocolli condivisi di intervento, necessari per fare in modo che le azioni messe in atto siano uguali per tutti.

L'Istituto continuerà a proporre e favorire, come già fatto in passato, momenti formativi dedicati all'integrazione delle TIC nella didattica, di gruppo nel caso della presenza di formatori esterni o sotto forma di tutoraggio personale realizzato dai docenti interni esperti (Team tecnologico).

- per gli studenti:

- discussioni in classe della policy nei primi giorni di scuola secondo modalità che variano a seconda dell'età dei ragazzi; inserire un estratto di questo documento nel diario scolastico di ciascun alunno, in particolare riferendosi ai comportamenti da attuare in caso di bisogno;
- proseguimento della collaborazione con esperti del settore (psicologi, Polizia Postale, associazioni attive, ...) per dare ai ragazzi l'opportunità di confrontarsi con delle figure competenti e autorevoli. Lo scopo è quello di evitare demonizzazioni del mezzo di comunicazione, ma nel contempo educare i ragazzi, con l'indispensabile supporto delle

famiglie, a conoscere i rischi che si nascondono nella rete e ad assumere atteggiamenti responsabili che li minimizzino, indirizzandoli verso un utilizzo consapevole di Internet mediante la diffusione della cultura della sicurezza in rete e prevenendo la diffusione dei fenomeni legati a cyberbullismo e adescamento online;

- momenti di confronto e discussione fra pari con studenti delle scuole superiori che hanno approfondito queste tematiche al punto di essere in grado di riportarle ai ragazzi di età inferiore, attraverso l'alternanza scuola-lavoro.

- per i genitori:

- organizzazione di incontri di sensibilizzazione sul tema della sicurezza informatica e di informazione circa i comportamenti da monitorare o da evitare. Tali incontri dovranno svolgersi possibilmente con la presenza degli addetti ai lavori: docenti, Polizia Postale, psicologi, personale specializzato appartenenti ad associazioni o enti preposti (Promeco, Cooperativa Sociale Girogirotondo Onlus etc.);
- inserimento all'interno del sito scolastico di materiali sull'argomento dedicati ad alunni e famiglie che possano essere di facile fruibilità e comprensione (brevi video esplicativi contenenti i rischi sociali e penali di determinate azioni, FAQ, presentazioni, etc.) e di link che rimandino a forum dove i genitori possano scambiarsi consigli o porre domande.

Ostellato, 22 novembre 2017

La Dirigente Scolastica

Dott.ssa Antonietta Allegretta

L'Animatore Digitale dell'Istituto Comprensivo

Ins. Rita Zironi

Gruppo Sicurezza sul Web

Ins. Mariagrazia Tiberio (Referente)

Ins. Maria Rita Sartori

Ins. Roberta Rossi

Ins. Adriana Martinello

Ins. Davide Caldironi