Policy di E-Safety

	Nome della scuola	Istituto Comprensivo Olgiate Comasco
	Data di revisione della Policy	novembre 2016
	Data della prossima revisione della Policy	settembre 2017
	Chi rivede la policy	• Dirigente scolastico • Animatore Digitale 2017/19 • Team per l'innovazione 2017/19 • Rappresentanti genitori CI • rappresentanti studenti secondaria (per la parte loro dedicata)

L'**Istituto Comprensivo Olgiate Comasco**, in base alle linee guida delle politiche nazionali, ha elaborato questa
Policy di e-safety (Uso Accettabile e Sicuro di internet e le LAN - reti locali e device).

Gli organi collegiali della scuola lo hanno approvato definitivamante[1] il 23 novembre 2016
Il documento inoltre è revisionato su base annuale.

Prima di firmarlo tutti i soggetti in causa devono leggerlo attentamente insieme a tutti gli annessi per accertarsi di averlo compreso in tutte le sue parti e di accettarne i contenuti.

Questa versione della Policy di e-safety è stata approvata dal

Collegio Docenti congiunto del 30 giugno 2016

e dal Consiglio d'Istituto del 23 novembre 2016

[1] Attenzione: le parti che si possono attuare da subito sono scritte in nero.
Alcune parti di questo documento sono scritte in grigio chiaro poiché in questo momento non possono essere attuate così come dichiarate. Si prevede la messa in opera e la realizzazione dei suddetti punti gradualmente nei singoli plessi e nell'arco dell'anno scolastico, con la collaborazione di tutti gli stakeholders.

INDICE

APPARATI (da considerarsi parte integrante di questo documento e messi in allegato separato):

1. Procedure operative per la gestione delle infrazioni alla Policy.
2. Procedure operative per la protezione dei dati personali.
3. Procedure operative/pratiche ad esempio per la rilevazione, il monitoraggio e la gestione delle segnalazioni e gestione dei casi.
4. PUA (Policy di utilizzo accettabile delle TIC e Internet) per le diverse età e ruoli

CREDITI:

Questa Policy è stata scritta attingendo, studiando, modificando e adattando ricerche e materiali presi da:

- Generazioni Connesse, ***SIC Safer Internet Centre Italiano*** - progetto finanziato dalla Commissione Europea nell'ambito del programma The Connecting Europe Facility (CEF) - Safer Internet, per la promozione di strategie finalizzate a rendere Internet un luogo più sicuro per gli utenti più giovani, indicando modalità e prudenze per uso positivo e consapevole. Il progetto è coordinato dal MIUR, in partenariato col Ministero dell'Interno-Polizia Postale e delle Comunicazioni, l'Autorità Garante per l'Infanzia e l'Adolescenza, Save the Children Italia, Telefono Azzurro, Università degli Studi di Firenze, Università degli studi di Roma "La Sapienza", Skuola.net, Cooperativa E.D.I. e Movimento Difesa del Cittadino.
Generazioni Connesse, nella persona di **Valeria De Natale** ci ha supportato nella stesura, revisione, pubblicazione di questo documento e dei suoi apparati

- London Grid For Learning motto:*"Lavoriamo insieme per una scuola leader nelle nuove tecnologie"*, consorzio finanziato delle autorità locali di Londra e 2.500 scuole che lavorano insieme per fornire numerosi servizi al costo effettivo delle TIC (es. servizi di gestione dati e navigazione sicuri, affidabili; fornire documenti di indirizzo e modelli di documenti riguardo ai problemi di e-safety; materiali didattici di alta qualità) Abbiamo usato i contenuti offerti da questa organizzazione rispettando Terms and Conditions of Use for LGfL Services and Resources

- Regolamenti degli Istituti Comprensivi di Merate (Lecco) D.S. prof. **Alberto Ardizzone** e di Arcola-Ameglia, D.S. prof. **Antonio Fini**

- *Navigazione sicura e consapevole* pagina e contenuti curati dall'insegnante **Paola Limone**, Direzione Didattica Rivoli 1 (To)

- Rete Piemontese Rupar, *Testo base della PUA,* il cui contenuto si può visionare a questo link

1. Introduzione e Panoramica

1.1 Fondamento e Scopo della Policy

Sia a livello internazionale, che nel contesto italiano, la presenza sempre più diffusa delle tecnologie digitali nella vita di tutti i giorni dei più giovani apre nuove opportunità ma pone nuove attenzioni dal punto di vista del loro uso sicuro, consapevole e positivo.
Negare questa evidenza, sarebbe come non considerare la realtà in cui viviamo.
Il Piano Nazionale Scuola Digitale[2] delinea in modo esplicito che a scuola si devono imparare, consolidare, rafforzare competenze digitali[3] tali da permettere agli alunni, futuri cittadini, un loro uso sempre più proficuo e consapevole[4]. Inoltre, lo sviluppo e l'integrazione dell'uso delle TIC[5], ed in particolare di Internet, nella didattica offrono le condizioni e l'occasione per una trasformazione concreta della relazione insegnamento/apprendimento e un'adesione al reale.

A partire da queste considerazioni, nasce questa e-Safer Policy[6] , dove si delineano:

- 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 dall'ambiente scolastico 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, infine, è un documento programmatico che impegnerà la scuola e i suoi attori anche per gli anni futuri: di conseguenza quanto si troverà di

[2] PNSD, Decreto n. 851 del 27-10-2015
[3] http://www.agid.gov.it/agenda-digitale/competenze-digitali/competenze-base
[4] Indicazioni Nazionali 2011 - prot. n. 7734 26 novembre 2012, pag. 11:
La competenza digitale consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Essa implica abilità di base nelle tecnologie dell'informazione e della comunicazione (TIC): l'uso del computer per reperire, valutare, conservare, produrre, presentare e scambiare informazioni nonché per comunicare e partecipare a reti collaborative tramite Internet.
[5] TIC, 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.
[6] Per *e-Safer 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.

seguito scritto sarà realizzato gradualmente nel tempo[7], 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[8].

Dettaglio degli scopi di questa policy:

- impostare i **principi fondamentali** che ci si aspetta e che verranno condivisi da tutti i membri della comunità scolastica rispetto all'uso delle TIC.
- **salvaguardare e proteggere** i bambini, i ragazzi e tutto il personale.
- assistere il personale della scuola per lavorare in modo sicuro e responsabile con Internet e altre tecnologie informatiche e di comunicazione
- monitorare i propri standard e le prassi.
- impostare **chiare aspettative di comportamento** per un uso accettabile e responsabile di Internet a scopo didattico. Tali comportamenti saranno da praticare anche a livello personale fuori dall'ambito scolastico.
- avere **procedure chiare** per affrontare un **uso improprio** degli strumenti digitali o gli abusi online come il cyberbullismo[9]
- assicurarsi che **tutti i membri della comunità scolastica sono consapevoli** del fatto che i comportamenti illeciti o pericolosi sono inaccettabili e che verranno intraprese azioni appropriate, disciplinari e/o giudiziarie quando la situazione lo richiederà.
- ridurre al **minimo il rischio** di accuse fuori luogo o dannose fatte contro gli adulti che lavorano con gli studenti.

Le principali aree di rischio per la nostra comunità scolastica possono essere riassunte così:

Contenuti[10]

- L'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

[7] Gradualmente = per gradi ma in modo progressivo. *Si prevede a regime completo entro triennio 2016/2019*

[8] in particolare: MIUR, Ministero Istruzione Università Ricerca, Generazioni Connesse, Unione Europea dicastero Educazione

[9] Questi hanno come riferimento anche altre Policy della scuola, come le *Norme generali di comportamento*

[10] cfr. da *Glossario* messoci a disposizione di Generazioni connesse

- Validazione dei contenuti: come controllare l'autenticità e l'esattezza dei contenuti online
- Pornografia

Contatto[11]

- Grooming (adescamento online), sfruttamento sessuale
- Cyberbullismo e bullismo in tutte le forme
- Il furto di identità, comprese le password
- Pedopornografia (con questo termine si intende qualsiasi foto o video di natura sessuale che ritrae persone minorenni)

Condotta[12]

- I 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: 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), gioco d'azzardo o gambling, videogiochi online in comunità mondiali (alcuni rischi associati possono essere ad esempio: contatti impropri con adulti, contenuti violenti e/o inadeguati; acquisti incontrollati, ecc.), l'immagine del corpo
- Sexting
- Copyright (poca cura o considerazione per la proprietà intellettuale e i diritti d'autore)

1.2 A chi è rivolta?

Questa policy si applica a tutta la comunità dell'Istituto comprensivo di Olgiate Comasco

- ai bambini, che frequentano la scuola dell'Infanzia e la scuola Primaria;
- ai ragazzi della Secondaria di primo grado;
- a tutti i docenti che svolgono la loro attività di insegnamento nella nostra scuola, anche per brevi periodi;
- al dirigente scolastico e al dirigente dei servizi amministrativi;
- a tutto il personale amministrativo e a tutti i collaboratori scolastici indistintamente;
- a tutti gli operatori/professionisti e/o volontari che entrano a scuola - in particolare a quelli che si mettono in relazione con i nostri ragazzi (a titolo di esempio: educatori, esperti di progetto, assistenti di mensa, ecc…)

[11] ibidem
[12] ibidem

- ai genitori tutti
- ai visitatori/ospiti
- a tutti coloro che hanno accesso ai sistemi di connessione e usano qualsiasi strumentazione digitale della scuola o anche device[13] personali dentro e fuori dall'istituto comprensivo di Olgiate Comasco (in tutti i suoi 8 plessi).

1.3 Una Complessità da gestire e una riflessione da fare

Viviamo in un mondo misto dove locale e globale non sono due dimensioni alternative. Le nuove tecnologie *mettono in relazione* e la relazione mette in contatto reale e virtuale le persone: non c'è frattura tra virtuale e reale perché questi due mondi si compenetrano. L'uno *procede o prosegue* l'altro[14].

Gli strumenti tecnologici ci permettono questo e pervadono la nostra vita[15]: li portiamo in tasca, li vogliamo in classe, sono comodi, risolvono problemi; permettono di lavorare, di raccogliere e archiviare, di ricercare, di elaborare con pochi click e in sistemi condivisi con poca fatica.

Gli strumenti non sono né buoni né cattivi: questa distinzione dipende dall'uso che il singolo, il gruppo, la comunità intende farne.

Essendo la comunità scolastica un sistema complesso non si può vietare o liberalizzare *tout court* l'uso di sistemi tecnologici interconnessi: bisogna

---

[13] tratto da Wikipedia
Mobile Internet ***Device*** *(spesso abbreviato in MID) vengono indicati alcuni particolari* ***dispositivi*** *destinati soprattutto alla navigazione in Internet e pensati soprattutto per un pubblico non professionale.*

[14] Chiara Giaccardi, docente di Antropologia dei media all'Università Cattolica di Milano, *"Il contesto in cui ci stiamo muovendo è quello di un mondo "misto". Forse abbiamo già acquisito che il locale e il globale non sono due dimensioni alternative, ma sono compenetranti e non c'è l'una senza l'altra. Così come forse stiamo acquisendo il fatto che nel mondo "misto" in cui viviamo il reale e virtuale non sono in contrapposizione; anzi, il digitale ci può aiutare, potenziando la nostra capacità di azione, di comunicazione sul territorio, e rispetto agli incontri faccia a faccia la comunicazione digitale li precede e li prosegue. In più i social media consentono di arrivare ai lontani, ma anche di mantenere e vivere le relazioni con chi hai già vicino e che ha bisogno di essere accompagnato"*. intervento su "Le condizioni per una relazione autentica" - Seminario di studi «In 120 caratteri comunicare la Chiesa»

[15] Manuel Castells, *Galassia Internet*, traduzione di Stefano Viviani, Feltrinelli, Milano, 2007, p. 262 *"Immagino che qualcuno potrebbe dire: "Perché non mi lasciate da solo? Non voglio far parte della vostra Internet, della vostra civiltà tecnologica, o della vostra società in rete! Voglio solo vivere la mia vita!" Bene, se questa è la vostra posizione, ho delle brutte notizie per voi. Se non vi occuperete delle reti, in ogni caso saranno le reti ad occuparsi di voi. Se avete intenzione di vivere nella società, in questa epoca e in questo posto, dovrete fare i conti con la società in rete. Perché viviamo nella Galassia Internet."*

distinguere e fare delle differenze nel rispetto dello sviluppo delle competenze del singolo e delle tappe di crescita.
Mettiamo a fuoco allora la situazione.

Primo:
A scuola si può **usare la tecnologia con**

- strumenti (mobile e fissi) in modalità cablata e/o WiFi di proprietà dell'Istituto
- mezzi propri (smartphone/tablet/laptop) il cui **uso accettabile** in ottica di metodologia BYOD (Bring Your Own Device) può essere accolto perchè diventa opportunità didattica/professionale e viene strettamente regolato in seguito da questa policy.

Secondo:
A scuola **chi usa la tecnologia**

- attenzione **all'età e al ruolo *professionale* dell'utente** appartenente alla comunità scolastica

Terzo:
Nell'ambiente scuola si usa le **tecnologia per** e **quando**

- uso privato: **mai permesso liberamente ai minori**, è regolato secondo i profili di utenza per i maggiorenni o persone equiparate[16]
- uso **relativo alla propria *professione* nella comunità scolastica** che segue regole condivise di sicurezza, protezione, rispetto

Per la definizione di queste situazioni si rimanda al capitolo 4

1.4 Ruoli e Responsabilità

Ruolo	Responsabilità Chiave
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

[16] per *persone equiparate* si intende persone dai 16 anni in su, es. gli studenti dei corsi CPIA-Como che ha sede nel nostro istituto

	sicurezza di navigazione utilizzando *adeguati sistemi informatici e servizi di filtri Internet.* → ***Previsione ragionevole di adeguamento:*** *entro prossimo triennio tutto l'istituto con configurazioni diverse a secondo dell'utenza e dei bisogni formativi espressi.* • 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 garantire adeguate *valutazioni di rischio* nell'usare strumenti e TIC, effettuate in modo che comunque quanto programmato possa soddisfare le istanze educative e didattiche dichiarate nel PTOF di Istituto. • Ricevere le relazioni di monitoraggio periodiche della sicurezza online dal Coordinatore al termine di ciascun anno scolastico. • Garantisce che ci sia un sistema di monitoraggio della rete e personale di supporto che metta in atto procedure di sicurezza on-line interne in collaborazione con le successive figure di sistema. • Assicura che sito web della scuola includa informazioni sulla cultura della sicurezza online, rilevanti e condivise con i diversi stakeholders.
Team per la sicurezza online composizione: **A - Coordinatore della Sicurezza Online** + B - Animatore Digitale e Team per l'innovazione + C - Pronto soccorso digitale + 1 rappresentante per ogni plesso	• Il **coordinatore** e il **team della sicurezza** si fanno carico giorno per giorno della responsabilità dei problemi di sicurezza online e sono riferimento per la creazione e la revisione delle politiche di sicurezza online della scuola e dei relativi documenti. • Si impegnano a promuovere la cultura della sicurezza on-line in tutta la comunità scolastica. • Garantiscono che l'educazione all'uso consapevole delle TIC e alla sicurezza online sia inserita all'interno del curricolo di studi dei bambini e dei ragazzi. • Il Coordinatore e il team devono garantire che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente di sicurezza on-line. • Collaborano, al bisogno e se è il caso, con il personale tecnico (anche esterno) in forza alla scuola scuola. • Il **coordinatore** comunica con il team e la componente *genitori* per discutere questioni,

(se non è già rappresentato da A, B, C) + *per consultazione:* referenti genitori indicati dal Consiglio di Istituto; 4 studenti volontari della Secondaria	esaminare i registri degli incidenti e *i registri di controllo di filtraggio/cambio per un aggiornamento adeguato.* • Il coordinatore promuove e facilita la formazione e la consulenza per tutto il personale. • Il coordinatore supervisiona qualsiasi sondaggio e feedback in materia di sicurezza online. • Al coordinatore vengono comunicate dal team situazioni di rischio o conclamate. Il coordinatore deve riferire tempestivamente al dirigente ed insieme possono prendere contatti con le Autorità Locali e agenzie competenti. • Viene periodicamente aggiornato in materia di sicurezza online e relativa legislazione, per aumentare la conoscenza relativa ai problemi di tutela dei minori.
Coordinatore competenze digitali Animatore Digitale	• Garantisce l'inserimento dell'educazione alla sicurezza online come cardine nello sviluppo delle competenze digitali (educazione alla cittadinanza digitale).
Network Manager Responsabile Sicurezza Internet di Istituto in collaborazione - per le parti di pertinenza - referenti di plesso per l'informatica e le infrastrutture	• Segnala problemi relativi alla sicurezza online rilevati al Coordinatore per la sicurezza online. • Gestisce i sistemi informatici della scuola, assicurando che: - la policy di **sicurezza password** sia rigorosamente rispettata. - tutti i sistemi **per il rilevamento di usi impropri** e di attacchi/minacce intenzionali (ad esempio mantenendo la protezione antivirus) sono attivi *- applica, mantiene e integra in modo regolare e con opportuni interventi concordati con il coordinatore la policy della scuola sul web filtering.* • Si tiene aggiornato sulla policy di sicurezza online della scuola e condivide le informazioni tecniche al fine di svolgere efficacemente il proprio ruolo di t*ecnico della sicurezza online* e informa e aggiorna tempestivamente Dirigente Scolastico e Coordinatore dei problemi rilevati. • Garantisce che l'uso della TIC della scuola e le piattaforme online dell'istituto siano regolarmente monitorate e che qualsiasi abuso/uso improprio o qualsiasi tentativo relativo ad essi è segnalato al coordinatore per la sicurezza online e al Dirigente

	Scolastico. • Garantisce che appropriate procedure di backup e piani di disaster recovery siano in atto (anche da parte di terze parti). • Mantiene aggiornate le documentazioni delle procedure tecniche di sicurezza on-line della scuola.
Manager dei dati e delle informazioni **DS e Dsga**	• Garantisce che i dati di gestione siano accurati e aggiornati. • Garantisce le migliori pratiche nella gestione delle informazioni, vale a dire che: mette in atto un sistema di controllo di accesso appropriati; i dati sono utilizzati, trasferiti e cancellati in linea con i requisiti di protezione dei dati. • mantiene i controlli di accesso per proteggere le informazioni personali e sensibili archiviati su dispositivi di proprietà della scuola.
Insegnanti	• Leggono, capiscono, firmano e aderiscono alla Policy di utilizzo (riassunta anche in una PUA = Policy di Usabilità accettabile dedicata). • Educano alla sicurezza online nello svolgersi curriculum della propria disciplina. • Supervisionano e guidano gli alunni con cura quando sono impegnati in attività di apprendimento che coinvolgono tecnologie online. • Garantiscono che gli alunni siano capaci di ricercare contenuti online in sicurezza e siano pienamente consapevoli dei problemi relativi ai contenuti elettronici (come ad esempio le leggi sul copyright). **Strategia d'uscita** Alla fine del periodo di lavoro o per periodi di sospensione: si deve restituire qualsiasi apparecchiatura o dispositivo in prestito dalla scuola. Questo includerà anche la riconsegna di numeri PIN, ID e password per consentire ai tecnici di intervenire sui dispositivi per il resettaggio. Si indicherà una data di fine accesso ai propri account di Istituto (GS4E e sito - di norma un mese dal fine rapporto) per consentire il salvataggio di dati personali.
Tutto il personale dell'istituto, gli educatori, gli esperti esterni	• Devono leggere, comprendere, aderire alla Policy di sicurezza (riassunta anche in una PUA = Policy di Usabilità accettabile dedicata) e aggiornarsi sulle relative modifiche. • Devono segnalare qualsiasi abuso sospetto o

e i volontari	qualsiasi problema al coordinatore della sicurezza on line. • Hanno consapevolezza delle problematiche di sicurezza online prese in esame dalla scuola con questo documento. • Assumono comportamenti sicuri, responsabili e professionali nell'uso delle tecnologie **Strategia d'uscita** Alla fine del periodo di lavoro o per periodi di sospensione: si deve restituire qualsiasi apparecchiatura o dispositivo in prestito dalla scuola. Questo includerà anche la riconsegna di numeri PIN , ID e password per consentire ai tecnici di intervenire sui dispositivi per il resettaggio. Si indicherà una data di fine accesso ai propri account di Istituto (GA4E e Sito -di norma un mese dal fine rapporto) per consentire il salvataggio di dati personali.
Bambini e ragazzi	• Leggono, capiscono, firmano e aderiscono alla Policy di utilizzo (riassunta anche in una PUA = Policy di Usabilità accettabile dedicata) ogni anno. • Capiscono l'importanza di segnalare l'abuso, l'uso improprio o l'accesso a materiali inappropriati. • Sanno quali azioni intraprendere se loro o qualcuno che conoscono si sente preoccupato o vulnerabile quando utilizza la tecnologia online. • Capiscono l'importanza di adottare sempre comportamenti sicuri e buone pratiche di sicurezza online quando usano le tecnologie digitali e sono consapevoli che la policy di sicurezza online della scuola può aiutarli anche fuori dalle mura e/o dall'orario scolastico. • Contribuiscono con sondaggi a raccogliere informazioni delle loro esperienze online e con suggerimenti al miglioramento di tutte le parti di questo documento e/o dei documenti ad esso correlati dove sono direttamente coinvolti.
Genitori	• Leggono, capiscono, approvano, firmano e promuovono facendola propria la Policy di sicurezza online che la scuola contrae con il/i loro figlio/i (riassunta anche in una PUA = Policy di Usabilità accettabile dedicata) • Si consultano con la scuola (Coordinatore sicurezza online/Dirigente/Team per la sicurezza) se hanno preoccupazioni circa l'uso della tecnologia online o

	offline da parte dei loro figli. • Sostengono la scuola nel promuovere la sicurezza online e approvano un accordo sull'uso accettabile delle tecnologie - che può comprendere anche l'uso concordato di device personali, di Internet *attraverso la rete di istituto* e l'uso da parte della scuola di immagini fotografiche e video ai fini di promulgazione/documentazione didattica e partecipazione a progetti/concorsi promossi da Enti di affermata reputazione in ambito educativo o territoriale.
Gruppi esterni, enti educativi	• Ogni individuo/organizzazione esterna all'istituto è tenuto a conoscere questa Policy prima di utilizzare la tecnologia o Internet della scuola all'interno e fuori dall'edificio scolastico e se sarà possibile firmerà i Protocollo di "Usabilità accettabile" (PUA) coerente con il profilo della sua utenza. Sostiene l'istituto nel promuovere la sicurezza online. • Mette a sistema un'adeguata educazione a agire comportamenti sicuri, responsabili e positivi nell'uso della tecnologia e degli spazi online dell'Istituto.

1.5 Condivisione e comunicazione della Policy all'intera comunità scolastica

La policy sarà comunicata al personale/alunni/comunità e persone che usufruiscono del nostro servizio di istruzione/educazione nei seguenti modi:

- sul sito della scuola una volta approvata in modo definitivo
- negli spazi di riunione e uffici dell'istituto
- nelle bacheche delle classi e negli spazi pubblici (atrio)
- via mail a tutti gli stakeholders con posta @icocscuole.it

Per il nuovo personale e i nuovi alunni:
Sarà comunicato con tutti i documenti da sottoscrivere all'atto della stipula del contratto/iscrizione.

Per tutto il personale sono previsti regolari aggiornamenti e nuova formazione in materia di sicurezza online.

Sono presi accordi di *utilizzo accettabile* secondo il calendario:
- degli organi collegiali con il personale (collegio settembre),
- degli studenti (settembre/prime due settimane di ottobre),
- dei genitori all'inizio di ogni anno scolastico (riunioni ottobre) .

In definitiva gli accordi d'uso accettabile verranno comunicati all'intera comunità scolastica all'inizio di ogni anno scolastico (entro ottobre).

1.6 Gestione delle infrazioni alla Policy

- La scuola prenderà e manterrà nel tempo tutte le precauzioni necessarie e adatte per garantire agli studenti l'accesso a materiale e ambienti appropriati, anche se è impossibile evitare in assoluto che essi trovino materiale indesiderato navigando su un computer della scuola.
  La scuola non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dall'accesso ad internet.
- Il Coordinatore della sicurezza online è la prima persona da contattare per qualsiasi incidente
- Qualsiasi sospetto, rischio, violazione va segnalato in giornata al Coordinatore per la sicurezza online che riferisce al Dirigente.
- Qualsiasi allerta di uso improprio del personale va sempre riferito direttamente al Dirigente Scolastico, a meno che esso si riferisca al Dirigente Scolastico stesso; in questo caso si riferisce direttamente alle autorità di competenza.
- Al personale, agli studenti e agli altri componenti della comunità scolastica sono date informazioni sulle infrazioni previste e le eventuali sanzioni.
- Le **sanzioni** riferite soprattutto agli alunni avranno come **carattere preferenzial**e quello **educativo/riabilitativo** e in ogni caso verrà **coinvolta la componente genitori, in qualità di primi educatori.**

1.7 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.

1.8 Integrazione della Policy con Regolamenti esistenti.

La e-safety policy fa riferimento e si armonizza con tutti gli altri regolamenti vigenti nell'Istituto in particolare con le *Norme generali di comportamento* con relativa tabella di sanzioni previste.

Va a integrare tale regolamento costituendo la sezione relativa all'*uso delle nuove tecnologie, dei nuovi ambienti di apprendimento e metodologie didattiche* offerti dall'Istituto (es. Aule Smart- PON 2012/2020, didattica BYOD, GS4E learning enviroment/sistema di cloud computing).

Tutto ciò che qui non è normato è da considerarsi regolamentato secondo tale disciplina generale.

2. Formazione e Curricolo

2.1 Safety digital skills: curricolo per gli studenti

Questa scuola dall'anno scolastico 2016/2017
definisce un chiaro e progressivo programma di educazione alla sicurezza online e uso delle TIC:

- è parte integrante del programma di sviluppo delle competenze digitali e di cittadinanza digitale;
- abbraccia una vasta gamma di abilità e di comportamenti auspicabili legati all'età e all'esperienza dei ragazzi;
- delinea azioni per l'uso attento degli strumenti online al fine di garantire che siano adeguati all'età dei ragazzi e sostiene gli obiettivi di apprendimento in aree curricolari specifiche individuate dai docenti;
- ricorderà agli studenti le loro responsabilità attraverso le PUA (Policy/accordo di uso accettabile)
- assicura il personale docente e non che i ragazzi sono consapevoli della loro responsabilità e che di conseguenza sono in grado di assumere un comportamento sicuro e responsabile nell'utilizzare la tecnologia (ad esempio, uso di password , la registrazioni, connessione e disconnessione sicura di login e logout , l'uso di contenuti , capacità di ricerca , diritti d'autore ...)
- esso assicura che i docenti e gli alunni conoscano i problemi intorno plagio; sanno come controllare il copyright e sanno anche che devono rispettare e riconoscere i diritti di proprietà intellettuale e il diritto d'autore;
- esso assicura che gli studenti utilizzano solo sistemi scolastici approvati e che pubblichino all'interno di ambienti adeguatamente protetti e garantiti, adatti alla loro età, in modo rispettoso ed essendo rispettati nella loro dignità.

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

In conformità al PNSD, il nostro istituto ha individuato:

Animatore Digitale triennio (2016/2019)[17]:
ins. Angela Mantovani (triennio 2017/2019)

il **Team per l'Innovazione (2016/2019)[18]**:
ins. A.M. Bartesaghi (scuola dell'Infanzia),
prof. Franca Vitelli (Scuola Secondaria),
prof. Francesca Ferrario (Scuola Secondaria).

[17] Nota prot. n 17791 del 19/11/2015
[18] Nota ministeriale prot. n. 4604 del 3/03/2016

Finalità di coordinare, proporre, organizzare proposte di formazione, eventi, percorsi didattici innovativi (es. metodologia Flipped, ESA, PBL ecc…)[19]

Gruppo di lavoro IDANT
(**I**nnovazione **D**idattica **A**ssistita dalle **N**uove **T**ecnologie)
composto (2015/16) da un insegnante per plesso (ad eccezione delle scuole dell'Infanzia)
Questo sta lavorando su:

Curricolo coding
Curricolo competenze digitali
e-Safety Policy

Questo Istituto si impegna a:

- formare i docenti su nuove metodologie di insegnamento/apprendimento attraverso percorsi di ricerca/azione e con attenzione al saper gestire didatticamente gli strumenti hardware, software, social, cloud computing individuandone punti di debolezza/forza anche in termini di sicurezza.

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

Questo Istituto si impegna a:

- dare formazione regolare al personale della scuola in materia di sicurezza online e a renderlo partecipe del il programma di educazione alla e-Safety;
- 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 e relativa PUA.

2.4 Sensibilizzazione/formazione delle famiglie.

Questo Istituto, in collaborazione con il Comitato genitori, si impegna a:

- formare/informare i genitori sulle problematiche legate alla sicurezza online e all'uso delle TIC.

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

La scuola gestisce linee internet dedicate esclusivamente alla didattica (in tutte le sedi) e una linea esclusiva per la parte amministrativa.
Lo stesso accade per per gli ambienti online: il sito istituzionale è distinto dall'ambiente online di apprendimento/organizzazione interna (GS4E).

[19] cfr. piano per il triennio 2016/2019 presentato dall'animatore Digitale e inserito nel PTOF aggiornato e riproposto annualmente.

Il sito istituzionale viene integrato da altri due ambienti i cui dati sono di nostra proprietà ma sono mantenuti e ne viene garantita la sicurezza da terzi: il registro digitale (Madisoft) e la segreteria digitale (Gruppo Spaggiari Parma)

3.1 Accesso ad internet, filtri, antivirus

*La nostra scuola ha in programma[20] un progressivo adeguamento di **filtraggio per l'accesso a internet** e un **sistema di autenticazione personale** per accesso alla rete (soprattutto per accesso al WiFi con propri device). Questo adeguamento non è di facile attuazione essendo distribuiti su più sedi con bisogni didattici diversi (8 plessi in tre comuni, le utenze, soprattutto alla secondaria sede CPIA, sono molto disomogenee).*

In una prima fase[21] si procederà ad adeguare in modo adeguato alle esigenze di sicurezza e di didattica la Secondaria, il plesso di San Gerardo e il plesso di Beregazzo con Figliaro in quanto soggetti a progetti Smartclass-PON

Il nostro Istituto si impegna a:

- informare tutti gli utenti che l'uso di Internet/e-mail istituzionali @icocscuole.it è monitorato nel rispetto della legge sulla Privacy;
- ad avere una connettività ragionevolmente sicura [a diverse bande e entro il 2020 si spera a banda larga] e filtrata (blocco siti con contenuti rivolti ad adulti, di gioco d'azzardo, odio razziale ecc.) definita in una policy di filtraggio[22];
- tutte le modifiche alla policy di filtraggio decise dal *team per la sicurezza digitale* vengono registrate e sono a disposizione solo del personale.
- assicura sistemi Antivirus OS o free aggiornati sui device di proprietà dell'Istituto.

3.2 Gestione accessi (password, backup, ecc.) e uso strumenti personali.

Questa scuola si impegna a:

Utilizzare singoli certificati di login per tutti gli utenti;

- *Utilizzare account guest di tanto in tanto per i visitatori esterni o a breve termine per l'accesso temporaneo ai servizi appropriati;*
- Utilizzare, dove sia possibile e preventivamente concordato, strumenti OS di controllo di gestione *a distanza* [controllo remoto - MDM] da parte dell'insegnante per il controllo di stazioni di lavoro/ tablet/visualizzazione di utenti/applicazioni e siti web.
- *installare eventuali software per il monitoraggio delel reti locali (rete LAN);*

[20] a regime entro il 2019
[21] ragionevolmente entro la fine del 2017
[22] Per la definizione della Policy di filtraggio faremo riferimento alle politiche della Rete Piemontese Rupar (Rete Unitaria Pubblica Amministrazione Regionale) o alle proposte di enti di Ricerca Universitaria (es. Università di Tolosa)

- avere un sistema automatico di backup dei dati del sito della scuola (Dati e database);
- Stoccare tutti i dati in modo conforme ai requisiti dell'Unione Europea e dell'Italia in termini di protezione/conservazione (*all'interno dell'UE o è comunque garantito secondo standard accolti da UE -es. accordi tra Google ed UE-*).

Per garantire che la rete venga utilizzata in modo sicuro, questa scuola:

- si assicura che il personale abbia letto, formato fatto propria e sottoscritta la Policy di sicurezza online adottata. Solo a seguito di ciò viene dato accesso alla posta elettronica e l'accesso alla rete. L'accesso ai servizi online avviene attraverso username unici e password. *Le stesse credenziali di nome utente verranno utilizzate per accedere alla rete locale della scuola.* L'utente si impegna a non cedere a nessuno le proprie credenziali/password.
- dà a tutti gli alunni della secondaria e, su richiesta degli insegnanti, agli alunni della primaria, un proprio nome utente e password che darà loro accesso *a Internet via accesso dell'Istituto (dove è previsto)* e altri servizi come la Google Suite for Education;
- chiarisce che nessuno dovrebbe accedere con un nome utente non suo ai servizi e dichiara che gli studenti non devono mai essere in possesso dei dati di login degli insegnanti e del personale;
- chiarisce che è necessario che tutti gli utenti si disconnettano quando hanno terminato il lavoro o sono obbligati a lasciare il computer incustodito.
- ribadisce che si dovrebbe lavorare online attraverso una navigazione in incognito.
- fa divieto di utilizzare sessioni lasciate per errore aperte da utenti precedenti. In tali casi è obbligatorio uscire dalla sessione (logout) ed informare l'utente.
- assicura a tutte le apparecchiature di proprietà della scuola una adeguata protezione antivirus e firewall.
- richiede che ogni apparecchiatura connessa alla rete disponga di una adeguata protezione antivirus.
- chiarisce che il personale deve assicurare che qualsiasi computer desktop o portatile dalla scuola in prestito di utilizzo, è fruito a supporto della sua funzione professionale.
- mantiene tali attrezzature in buono stato e in sicurezza;
- assicura che l'accesso alle risorse di rete della scuola da postazioni remote da parte del personale è controllato e limitato e che tale accesso avvenga solo attraverso sistemi LAN approvati;
- non consente ad alcuna agenzia esterna di accedere in remoto alla propria rete salvo che non vi sia una chiara necessità professionale; in questo caso l'accesso sarà limitato nel tempo e garantito attraverso sistemi approvati;
- Utilizza sistemi di disaster recovery che comprendono, uno spazio remoto backup: dati sito settimanale e giornaliero, GS4E in automatico,

segreteria digitale garantito da Spaggiari; registro elettronico garantiti da Madisoft.

- Questa scuola utilizza il trasferimento e mantenimento sicuro dei dati (pec o in modalità crittografata).
- Assicura che tutti i dati sensibili degli allievi o del personale inviati via Internet vengano crittografati o inviati e archiviati con sistema sicuro (pec o in modalità crittografata).
- *La nostra rete wireless assicura standard di sicurezza adatti per l'uso didattico.*
- Tutte le TIC e i sistemi di comunicazione sono stati installati da professionisti del settore e sono regolarmente verificati per assicurare che soddisfino gli standard di salute e sicurezza.

3.3 Password

Questa scuola chiarisce che:

- il personale e gli alunni devono sempre mantenere la propria password privata, non deve essere condivisa con gli altri;
- Se una password risulta compromessa o dimenticata si deve notificare subito alla segreteria o all'amministratore sito/GS4E che provvederà ad una sua sostituzione
- Tutto il personale ha il proprio nome utente e password univoci privati per accedere ai sistemi scolastici.
  Il personale ha la responsabilità di mantenere la(e) propria password(s) privata(e).
- La password deve garantire uno standard minimo di sicurezza: pertanto è obbligatorio formarla con almeno 8 caratteri alfanumerici, con maiuscole e minuscole.
- Sarebbe auspicabile cambiare le proprie password di accesso almeno 4 volte all'anno (ogni 3 mesi). È obbligatorio in caso di intrusione sospetta ai dati personali.

3.4 E-mail

Questo istituto ha attivato le GS4E:

- offre un account personale di posta elettronica @icocscuole.it (**I**stituto **C**omprensivo **O**lgiate **C**omasco **S**cuole) a tutti gli utenti adulti per uso professionale e raccomanda di tenere separata la e-mail privata da quest'ultimo.
  Il settaggio delle mail e delle app attive per ciascun account è differenziato secondo il profilo professionale dei singoli (organizzazioni interne alle GS4E).
- ogni ragazzo delle medie avrà un account personale, legale e senza alcun tipo di filtraggio o pubblicità.
- Questo verrà blindato attraverso un'opportuna personalizzazione da parte dell'amministratore dell'intera organizzazione (GS4E) che ne blocca

alcuni servizi[23] e non permette il contatto al di fuori dei membri del dominio icocscuole.it
- Per i bambini delle primaria l'account verrà attivato solo su richiesta esplicita dell'insegnante. Tali account saranno blindati e con app limitate.
- Farà in modo che la posta elettronica e gli account siano mantenuti e aggiornati nel tempo.
  Questi verranno disattivati dopo un mese dal giorno di cessato *rapporto di lavoro* con l'istituto (vale sia per gli alunni che per il personale)

L'Istituto si metterà in contatto con gli organi di Polizia Postale nel caso in cui qualcuno appartenente alla nostra organizzazione (alunno, docente, personale) riceverà e-mail che consideriamo particolarmente preoccupanti o che infrangano la legge.

Alunni:

- Agli alunni verranno insegnate le prudenze da attuare circa la sicurezza online e verrà discussa una *netiquette* di utilizzo della posta elettronica e ambienti elearning, sia a scuola che a casa.

Personale:

- Il personale utilizzerà sistemi di posta elettronica GS4E per soli fini professionali.
- L'accesso a scuola ad account di posta elettronica personali esterni può essere bloccato.
- Non dovrà utilizzare la posta elettronica per il trasferimento di dati sensibili del personale o dei ragazzi.
  Dati soggetti a *privacy e sensibili* di norma non devono mai essere trasferiti via e-mail. Se non esiste una soluzione alternativa al trasferimento sicuro dei file, si dovrà provvedere in modi diversi come riferire di persona o attraverso cartaceo non condiviso.

3.5 Sito web della scuola, blog e spazi didattici

Il Dirigente Scolastico, supportato col Consiglio di Istituto e dallo staff del sito, si assume la totale responsabilità di garantire che il contenuto del sito web è accurato, accessibile, aggiornato.

- Il sito web della scuola è conforme ai requisiti di legge[24];
- La maggior parte del materiale è prodotto direttamente della scuola o attinto da una comunità di pratica Porte Aperte sul Web, che si occupa di fornire modelli OS e supporto gratuito e volontario alle scuole italiane per i propri siti;
- Quando viene pubblicato o linkato il lavoro di altri, si mettono gli accrediti alle fonti utilizzate e si indicano chiaramente l'identità o lo stato dell'autore;

[23] Indicazioni di Servizio Marconi USR Emilia Romagna prof. Roberto Bondi e prof. Luigi Parisi e DS Antonio Fini IC Arcola Amelia
[24] http://www.agid.gov.it/tags/siti-web-pa

- Fotografie pubblicate sul web non verranno mai nominate con nomi completi dei soggetti né avranno didascalie così composte.
- Non si useranno i nomi degli alunni quando verranno salvati file, immagini o tag nella pubblicazione sugli spazi web della scuola.

3.6 Cloud computing: l'ambienti cloud GS4E, il registro elettronico, la segreteria digitale

- Il caricamento di informazioni sullo spazio di apprendimento online della scuola o su registro elettronico/segreteria digitale è condiviso tra i diversi membri del personale in base alle loro competenze: ad esempio tutti gli insegnanti di classe possono caricare informazioni nelle loro aree di pertinenza;
  si utilizzano per questi gli ambienti protocolli di navigazione https.
- Fotografie e video caricati negli ambienti online della scuola saranno accessibili solo ai membri della comunità scolastica e non possono essere diffusi in qualsiasi altro spazio web.
- Se pubblicati in chiaro in spazi social open questi dovranno essere quelli ufficiali della scuola e la loro pubblicazione dovrà essere autorizzata ad hoc;
- A scuola, gli studenti possono caricare e pubblicare esclusivamente all'interno del sistema cloud di proprietà dell'Istituto.

3.7 Social network.

Personale, collaboratori, esperti, educatori

- Il personale è istruito e obbligato a mantenere sempre la comunicazione professionale separata da quella personale/privata.
- Gli insegnanti, esperti ed educatori sono formati a non organizzare a titolo personale spazi su social network da usare con gli studenti: questi devono essere autorizzati dalla dirigenza e devono riguardare progetti didattici di divulgazione e la documentazione dei processi di apprendimento.
- Gli insegnanti, esperti ed educatori sono formati a non aprire i loro spazi ai loro studenti: si devono usare i sistemi dedicati e istituzionali della scuola per tali comunicazioni.

L'uso di qualsiasi social networking approvato dalla scuola (leggasi: canali ufficiali youTube, facebook, twitter, Pinterest, Instagram ecc...) è normato secondo questa e-safety policy.

Il personale della scuola in uso *privato* di spazi social:

- non fa riferimento a studenti/alunni, genitori/tutori o personale scolastico;
- non dovrebbe essere *amico* online di qualsiasi alunno/studente.
- non entra in discussioni online su questioni personali relative agli stessi membri della comunità scolastica;
- non attribuisce opinioni personali alla scuola o alla sua dirigenza o alle autorità locali;
- non deve compromettere il ruolo professionale e non deve portare discredito all'Istituto con le sue opinioni personali.

Gli studenti

- Agli studenti vengono insegnati i comportamenti accettabili e di sicurezza da assumere sui social networking: come segnalare abusi, intimidazioni o vessazioni, atti di bullismo attraverso un apposito percorso di educazione all'uso sicuro dei social network.
- Gli studenti sono tenuti a firmare e seguire la nostra PUA alunni adattata alla propria età.

Genitori:

- I genitori vengono istruiti sui rischi di utilizzo dei social networking e i nostri protocolli attraverso una PUA genitori.

Materiali di comunicazione aggiuntiva sono stati organizzati in questa pagina del sito istituzionale di Istituto:
http://www.icolgiatecomasco.gov.it/cittadini-digitali/

3.8 Protezione dei dati personali: Sistema di gestione delle informazioni e trasferimento dati

Pratiche strategiche e operative

In questo Istituto[25]:

- Il responsabile del trattamento dei dati personali è dell'Istituzione scolastica, la responsabilità è esercitata dal dirigente scolastico.
- Il Dirigente Scolastico è il responsabile della gestione dei rischi relativi a questo ambito.
- Il Dirigente scolastico designa quali incaricati al trattamento dei dati il Direttore Sga e il personale amministrativo.
- il Direttore Sga, cui è conferito dal Dirigente il compito di sovrintendere/amministrare il sistema di gestione e custodia dei dati personali, individua gli incaricati del trattamento dei dati medesimi e ne

[25] Le segreterie delle Istituzioni scolastiche devono dotarsi di misure minime, di strumenti e amministratori di sistema, secondo quanto previsto dal D.P.R.318/1999

indica i criteri di gestione, attribuendo a ciascun incaricato un codice identificativo personale per l'utilizzazione dell'elaboratore.
- Il personale è istruito sulla procedura da seguire per segnalare eventuali incidenti dove la protezione dei dati potrebbe essere stata compromessa.

Soluzioni tecniche

- Il personale ha un'area protetta sulla rete per memorizzare i file sensibili (segreteria digitale e registro elettronico)
- Si richiede al personale di usare i sistemi di logout al momento di lasciare il computer usato e anche di far rispettare lockout (bloccaggio) dopo 10 minuti di tempo di inattività.
- Tutti i server sono in posizioni bloccabili e gestiti da personale interno
- la segreteria adotta: password;
  individua soggetti preposti alla gestione delle password;
  ha un codice identificativo personale per ogni utente;
  ha programmi antivirus;
  protegge e regolamenta gli accessi ai locali che ospitano i dati riservati o in cui si trovano le postazioni di lavoro che ne consentono l'accesso;
  definisce i criteri per garantire l'integrità dei dati;
  definisce i criteri per garantire la trasmissione sicura dei dati.
- La segreteria si dota di mezzi elettronici adeguati per impedire l'accesso dall'esterno alla rete della segreteria, quali FIREWALL od altri strumenti.
- *I dettagli di tutto l'hardware di proprietà della scuola saranno registrati in un inventario di hardware.*
- *I dettagli di tutti i software di proprietà della scuola saranno registrati in un inventario del software.*
- Lo smaltimento di qualsiasi apparecchiatura sarà conforme alle norme di smaltimento dei rifiuti elettrici ed elettronici.
- Per qualsiasi server che conteneva dati personali o soggetti alla tutela sulla privacy, cercheremo di ottenere un certificato di cancellazione sicura.
- *Useremo un software di eliminazione sicura dei file (eliminazione definitiva anche di file temporanei)*

Settaggio e accesso di strumenti mobile di proprietà della scuola

Il dispositivo è di proprietà della scuola e si accede con un unico account

- Il dispositivo dispone di un account creato dalla scuola e tutte le applicazioni e file di uso sono adeguate a queste regole di Policy.
- Nessun elemento personale può essere aggiunto a detto dispositivo.
- Il PIN di accesso al dispositivo non deve essere modificato per nessun motivo e deve essere sempre immesso e conosciuto dal gestore di rete.

4. Strumentazione personale: uso dei cellulari e dispositivi mobile (notebook, laptop, tablet)

Premessa alla sezione

Organizzeremo parte di questa sezione distinguendo queste ***tipologie di utenza***:

- **Bambini e ragazzi:**
  - **studenti** di età diverse.
- **Maggiorenni**
  - **docenti, operatori, esperti** ecc. che hanno responsabilità educative e didattiche e che lavorano a diretto contatto con i ragazzi.
  - **personale della scuola, genitori** e in generale **persone maggiorenni (si equiparano a questi ultimi anche i 16enni e 17enni)** presenti a vario titolo e in diversi momenti nello spazio dell'Istituto.

4.1 BYOD Bring Your Own Device[26]

La possibilità di portare a scuola propri device **(BYOD Bring Your Own Device)** è da considerarsi un'opportunità didattica e professionale.

Questa opportunità ci porta a considerare che:
Il loro uso a scuola da parte dei bambini e dei ragazzi **è concordato con genitori dagli insegnanti** che useranno tali strumenti in classe solo in funzione didattica.
Ogni altro uso -come vedremo- **è vietato.**

[26] Portare a scuola il proprio smartphone, tablet o altro dispositivo personale in questo caso risponde ad esigenze e finalità totalmente diverse da quelle assimilabili ad un uso privato. Esse si riferiscono allo svolgimento di attività didattiche innovative, collaborative o di sostegno al percorso didattico/lezione (es. foto di un oggetto che si stava copiando dal vero che serve per finire tavola in un secondo momento), che prevedano o che ammettano anche l'uso di dispositivi tecnologici. Queste situazioni rientrano in quelle opportunità che favoriscono negli alunni l'acquisizione di competenze digitali e di cittadinanza.
Cfr. #azione6 del PNSD: " La scuola digitale, in collaborazione con le famiglie e gli enti locali, deve aprirsi al cosiddetto BYOD (Bring Your Own Device), ossia a politiche per cui l'utilizzo di dispositivi elettronici personali durante le attività didattiche sia possibile ed efficientemente integrato".

4.2 Norme generali uso device mobili personali a scuola

- 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, svanisce nel nulla, viene danneggiato, vengono persi dei dati ecc.. la scuola non deve essere considerata responsabile della sicurezza di tali dispositivi/dati né deve farsi carico di eventuali risarcimenti;
- I dispositivi mobili **non possono essere utilizzati in alcune aree all'interno o di pertinenza dell'Istituto, ad esempio, spogliatoi e servizi igienici.**
  Vengono visualizzati cartelli di ***zona-mobile-free***.
- Qualsiasi dispositivo mobile (compresi smrtphone e tablet) utilizzato deve essere reso accessibile al monitoraggio e controllo da parte del Dirigente (o di chi in quel momento ne fa le veci) **come parte del normale monitoraggio/controllo delle attività scolastiche**; questi ha la possibilità di revocare o limitare l'autorizzazione d'uso in qualsiasi momento, se lo si ritiene necessario.
- 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.

4.3 Indicazioni generali per acquisizione di immagini e video digitali

In questa scuola:

- Chiediamo esplicito permesso dei genitori/tutore legale per utilizzare fotografie digitali o video che coinvolgono il loro figlio.
  Questa autorizzazione viene sottoscritta all'iscrizione o annualmente all'inizio delle attività didattiche.
- Ci impegniamo a non identificare alunni in materiali fotografici online o includere i nomi completi degli alunni nei titoli di qualsiasi cosa pubblicata e prodotta in video/DVD;
- Accettando e sottoscrivendo questa policy, i docenti si impegnano secondo le clausole dette nell'uso dei device personali per scattare foto/fare dei video ad alunni.
- L'istituto *prevede il blocco e/o il filtraggio ai siti di social networking* a meno che non vi sia uno specifico scopo educativo/didattico approvato.
- Gli alunni impareranno come le immagini possono essere manipolate nel percorso di educazione alla sicurezza online.
- Gli studenti saranno aiutati a riflettere sull'opportunità di pubblicazione di foto personali su qualsiasi spazio di rete social. Verranno informati su

come mantenere attive e alte le impostazioni di privacy e personali rispetto ad un possibile pubblico.

- Agli alunni viene insegnato che non devono pubblicare immagini, registrazioni audio o video di altri senza permesso. Verranno loro spiegati i rischi connessi al fornire informazioni attraverso le immagini (tra cui il nome del file), che rivelano l'identità degli altri e la loro posizione. Impareranno la necessità di mantenere i loro dati sensibili al sicuro e cosa fare se sono oggetti di stalking o abusi.

4.4 Per gli <u>studenti</u>: gestione degli strumenti personali - cellulari, tablet, laptop ecc.. ovvero i mobile device

Per poter sviluppare le competenze digitali in termini di consapevolezza, responsabilità e normalità -in linea con le Indicazioni nazionali per la scuola del primo ciclo- ma, come detto, anche per un'opportunità che può venire dall'uso dei **mobile device[27] personali** vogliamo distinguere **diverse situazioni didattiche**.

Prima di tutto ribadiamo queste raccomandazioni generali prescrittive:

- La scuola consiglia vivamente a tutti gli studenti di **non portare** telefoni cellulari e dispositivi mobile personali a scuola.
- Per le **scuole primarie** si vieta **ai genitori la possibilità di far portare a scuola ai loro bambini il telefono cellulare/tablet se non in casi speciali e sempre concordati con il corpo docente che ne delibera il modo di utilizzo** (quando, come, perché, per quanto tempo).
- **Per la scuola dell'infanzia il divieto è categorico.**
- La scuola accetta che ci possano essere circostanze eccezionali in cui un genitore può richiedere al Dirigente che suo figlio possa avere con se il telefono cellulare per problemi di sicurezza/salute.

[27] cfr. **BYOD**

- Se uno studente viola questa policy, il dispositivo verrà **in tutti i casi confiscato** e lo si terrà in un luogo sicuro in ufficio di segreteria.
  I dispositivi mobili saranno rilasciati solo ai genitori/tutore con delega secondo la tabella allegata[28].
- Telefoni e dispositivi non devono essere mai usati durante gli esami o prove nazionali.
  Questo porta alla esclusione dall'esame stesso e quindi all'immediata ripetizione dell'intero anno scolastico[29].
- Gli studenti sono responsabili della custodia del loro numero telefonico che non deve essere divulgato o gli ID/password personali. I ragazzi saranno guidati ad usare in modo appropriato e sicuro i loro smartphone/personal device e saranno istruiti sui limiti e le conseguenze di comportamenti non adeguati/non accettati.

Distinguiamo ora le due situazioni possibili:

Caso1

1. uso del telefono cellulare/tablet/altri dispositivi mobile personali ad **uso assimilabile al *privato*** per chiamate, sms, messaggistica in genere, gioco, ecc.

Caso2

2. ***BYOD:*** utilizzo delle funzioni, tipiche degli smartphone (foto, video, scrittura collaborativa e condivisione di documenti, varie applicazioni come le GA4E ecc...), comuni anche a tablet e altri dispositivi mobili (laptop o notebook), che possono avere una rilevanza e un possibile impiego nella didattica.

Chiariamo che: il caso 2 vale anche se i ragazzi stanno usando strumenti mobile di proprietà dell'istituto per le *attività didattiche a scopi professionali*[30].

Caso 1.
Uso privato per chiamate, sms, messaggistica in genere

Si ribadisce la puntuale applicazione della normativa vigente[31]: pertanto **l'uso di mobile device non è consentito** per ricevere/effettuare chiamate, SMS o altro tipo di messaggistica, giocare, ecc.

- Il divieto si applica all'orario delle lezioni e vale anche negli intervalli e nelle altre pause dell'attività didattica.
- L'estensione del divieto agli altri momenti di permanenza a scuola (intervallo, mensa, cambio dell'ora, ecc.), oltre a rispondere a necessità organizzative e di controllo, ha una motivazione educativa. Riteniamo

[28] cfr. Annessi 1
[29] Circolari annuali "Istruzioni sugli adempimenti per gli esami di stato del primo ciclo" di norma emanate nel maggio di ogni anno scolastico; cfr. Nota Ministeriale del 2010 Esami di Maturità e gestione TIC e device n. 3614 dell'11.5.2010
[30] L'alunno a scuola è considerato a tutti gli effetti un *lavoratore professionista*
[31] DPR 249/1998, DPR 235/2007, Direttiva Ministeriale 15.03.2007

infatti importante valorizzare momenti di relazione positiva tra gli studenti, evitando atteggiamenti di esclusione, di isolamento e di separazione dalla vita scolastica reale.
- Per quanto riguarda uscite, visite guidate e viaggi di istruzione, l'uso può essere consentito, se autorizzato dal docente, al di fuori dei momenti dedicati a visite guidate e attività legate all'aspetto didattico dell'uscita.

- La comunicazione con le famiglie, per qualsiasi urgenza, è sempre garantita attraverso il telefono della scuola[32].
- Le famiglie sono invitate a collaborare strettamente con l'Istituto, nello spirito della corresponsabilità educativa, evitando ad esempio di inviare messaggi o effettuare chiamate ai telefoni dei propri figli, durante l'orario scolastico o visite di istruzione.
- Se portati, gli alunni sono tenuti a mantenere i loro telefoni/device spenti e riposti in luogo non visibile durante l'intera permanenza a scuola, salvo quanto previsto nel caso 2 di questo paragrafo.
- Si deve severamente evitare di essere raggiunti da qualsiasi notifica o segnalazione, eventi particolarmente distraenti e disturbanti durante l'attività didattica.

Le contravvenzioni alle prescrizioni e divieti di cui a questo caso 1 sono sanzionate secondo quanto previsto alla sezione annessi n.1 e dalle Norme generali di comportamento di Istituto vigenti.

Caso 2. BYOD

Utilizzo delle funzioni che possono avere una rilevanza e un impiego nella didattica

In questo caso l'uso **di smartphone, tablet e altri dispositivi mobili personali , è consentito.**

Ricordiamo ai ragazzi che i device che usano sono *loro* solo nominalmente ma che, a tutti gli effetti, appartengono all'adulto che ha stipulato il contratto o li ha comprati.

- I dispositivi mobili personali verranno utilizzati unicamente durante le lezioni o il tempo scuola formale solo come parte di un'attività curriculare e secondo le modalità prescritte dall'insegnante e con **esclusiva finalità didattica**;
  in queste situazioni vanno comunque tenuti in modalità silenziata.
- Quando gli insegnanti faranno portare il device agli alunni questo dovrà essere caricato a casa.
- Nei momenti di non utilizzo, i device devono essere tenuti spenti (non è ammessa la modalità silenzioso) e debitamente conservati fuori dalla vista fin dall'arrivo a scuola.

[32] I docenti possono derogare a tale disposizione, consentendo l'uso del cellulare, in caso di particolari situazioni non facilmente risolvibili in altro modo.

Funzioni Bluetooth o similari dei dispositivi mobile devono essere spenti in ogni momento e non possono essere utilizzati per inviare immagini o file ad altri dispositivi mobili;
- Gli studenti non possono prendere in prestito dispositivi di altri studenti;
- *Per lavorare con strumenti di cloud computing*[33] *o più in generale se si ha necessità di essere collegati alla rete Internet, gli studenti potranno accedere alla rete* ***esclusivamente attraverso la connessione dell'Istituto*** *anche se si è dotati di accredito personale di navigazione, secondo le indicazioni date (vedi password e accreditamenti personali).* Non si deve fare uso di abbonamenti personali se non in casi di estrema necessità, valutati di volta in volta con l'insegnante di riferimento del processo didattico in corso.
- Immagini, video, registrazioni vocali possono essere effettuate previo consenso della persona o persone in questione e con l'autorizzazione dell'insegnante.
- I ragazzi devono chiedere l'autorizzazione prima di caricare/postare o condividere fotografie, video, registrazione audio o qualsiasi altra informazione che riguarda se e anche altre persone.
- Se uno studente ha bisogno di contattare i genitori o tutori, dovrà riferire ad un docente e potrà utilizzare un telefono della scuola.

Tenendo conto delle recenti indicazioni del Garante della privacy[34] , si ribadisce che la registrazione delle lezioni è possibile solo per usi strettamente personali e, pertanto, previe autorizzazioni di tutte le parti coinvolte.
La diffusione di tali contenuti è inoltre sempre subordinata al consenso da parte delle persone ritratte/riprese (minori e non; se minori l'autorizzazione va richiesta ai tutori legali/genitori) e della dirigenza della scuola.

Richiamiamo l'attenzione degli alunni sulle possibili conseguenze di eventuali riprese audio/video o fotografiche effettuate all'interno degli ambienti scolastici e successivamente diffuse con l'intento di ridicolizzare compagni o insegnanti o addirittura allo scopo di intraprendere azioni denigratorie, intimidatorie, vessatorie[35]. È infatti *bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità di sé e di altre persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati*[36].
Anche in questo caso si ravvisa la necessità di grande sintonia e collaborazione tra scuola e famiglia, in modo da favorire negli alunni lo sviluppo della necessaria consapevolezza e maturità nell'uso dei potenti strumenti ai quali hanno accesso.
In particolari casi, i consigli di classe/team o il dirigente scolastico potranno disporre specifiche condizioni d'uso, sia individuali che collettive, sempre con l'intento di ricondurre le sanzioni ad una finalità educativa e di ricercare attivamente forme di collaborazione con la famiglia.

[33] es. Classroom, spazio della scuole fornito dalle Google apps for education o Drive
[34] La privacy a scuola. Dai tablet alla pagella elettronica. Le regole da ricordare
[35] definite spesso con il termine di cyberbullismo
[36] cfr. Garante della privacy, La privacy a scuola. Dai tablet alla pagella elettronica. Le regole da ricordare

4.5 Per i <u>docenti, educatori, esperti di progetto</u>: gestione degli strumenti personali - cellulari, tablet ecc..

Norme generali

- Il personale non è autorizzato a utilizzare i propri telefoni cellulari o dispositivi a titolo professionale, come ad esempio per contattare i bambini, i ragazzi e le loro famiglie all'interno o al di fuori del proprio orario di lavoro e dall'Istituto.
  Tutti i visitatori sono invitati a mantenere i loro telefoni e dispositivi personali su silenzioso.
- La comunicazione Bluetooth dovrebbe essere in modalità nascosta o spenta.
  In ogni caso si deve evitare di essere raggiunti da qualsiasi notifica o segnalazione o eventi particolarmente distraenti e disturbanti la stessa attività didattica. I cellulari o dispositivi personali non dovranno essere utilizzati durante l'insegnamento a meno che non sia stato concesso un permesso dal Dirigente[37].
- Al personale verrà rilasciato un telefono di proprietà della scuola nel caso in cui è necessario poter contattare gli studenti, i genitori o altri accompagnatori.
- Se i Docenti hanno un motivo educativo/didattico per permettere ai ragazzi di usare telefoni cellulari o dispositivi mobili di loro proprietà, questo sarà possibile solo dietro approvazione Dirigente Scolastico.
- I docenti in linea di principio non devono utilizzare dispositivi di proprietà personale, come cellulari o macchine fotografiche, per scattare foto, video, registrazioni audio/video che coinvolgano gli studenti e preferenzialmente utilizzare solo le attrezzature adatte allo scopo di proprietà della scuola.
  Se la scuola non possiede tali attrezzature o esse sono di uso difficoltoso potrà utilizzare le proprie previo permesso del dirigente e seguire le norme di questa Policy scrupolosamente.
  Tale uso autorizzato deve essere possibilmente segnalato sul registro di classe.
- Gli insegnanti o persone maggiorenni *dovranno preferenzialmente accedere alla rete tramite accreditamento personale alla rete della scuola.*
  In caso di necessità possono fare uso di abbonamenti personali.
- In caso di emergenza il docente o qualsiasi altro membro del personale della scuola (compresi educatori ed esperti di progetto) se non ha accesso immediato e semplice a un dispositivo di proprietà della scuola, è autorizzato ad utilizzare il proprio cellulare stando attento a non divulgare

[37] es. Il Dirigente concede la compilazione del Registro elettronico con tablet di proprietà

dati sensibili o personali.
Dovrà poi riferire l'incidente al Dirigente Scolastico.

- Il personale della scuola può utilizzare il proprio telefono cellulare durante i periodi di pausa, seguendo le regole generali di non disturbo delle attività.
- Se un membro del personale è in attesa di una chiamata personale chiede un'autorizzazione specifica per poter utilizzare il suo telefono al di fuori dei momenti di pausa, esclusivamente in modalità silenziata.

- Chi non rispetta le regole della policy potrà subire sanzioni riportate negli Annessi n. 1 *Procedure operative per la gestione delle infrazioni alla policy*

Distinguiamo due casi:

Caso 1.
Uso per chiamate, sms, messaggistica in genere durante le attività di docenza per uso privato

- L'uso del cellulare/tablet non è consentito per ricevere/effettuare chiamate, SMS o altro tipo di messaggistica, giocare, durante l'orario di docenza/lavoro.
- Il divieto si applica anche negli intervalli e nelle in altre situazioni che per responsabilità sono assimilabili ad *attività didattica* come mensa, cambio dell'ora, intervalli.

Caso 2.
Utilizzo di funzioni che possono avere rilevanza in ambito della propria professione e un possibile impiego nella didattica nello svolgimento delle lezioni

L'uso di smartphone, tablet e altri dispositivi mobili è consentito con esclusiva finalità didattica e professionale.
Per lavorare con strumenti di cloud computing (come GS4E/Nuvola) o più in generale se si ha necessità di essere collegati alla rete Internet *dovrà essere usata preferibilmente la connessione dell'Istituto* anche se si è dotati di accredito personale di navigazione, secondo le indicazioni date nei paragrafi precedenti.

Ribadiamo ancora che le riprese -fotografiche, vocali, video- potranno essere eseguite solo per scopi didattici dichiarati, con il consenso delle parti interessate (obbligatoria liberatoria dei genitori o tutori), e tenendo conto delle recenti indicazioni del Garante della privacy[38].
Registrazioni o immagini effettuate durante lezioni, uscite didattiche o attività di presentazione *allargate* (come feste, eventi culturali ecc…) possono essere utilizzate per usi esclusivamente didattici, di divulgazione delle attività dell'istituto e di documentazione pedagogica.

[38] ibidem, La privacy a scuola. Dai tablet alla pagella elettronica. Le regole da ricordare

La diffusione di contenuti, da farsi solo sui canali ufficiali di proprietà della nostra scuola, è inoltre sempre subordinata all'autorizzazione del Dirigente Scolastico e, come detto, al consenso da parte delle persone ritratte/riprese.

Richiamiamo l'attenzione dei docenti, educatori, esperti sulle possibili conseguenze di eventuali riprese audio/video o fotografiche effettuate all'interno degli ambienti scolastici e successivamente diffuse con l'intento diversi da quelli dichiarati sopra o *che ledono la riservatezza e la dignità delle persone può far incorrere in sanzioni disciplinari e pecuniarie o in veri e propri reati*[39]

4.6 Per <u>personale della scuola</u>: gestione degli strumenti personali - cellulari, tablet ecc.

Caso 1.
Uso per chiamate, sms, messaggistica in genere durante le attività lavorative per uso privato

- L'uso del cellulare/tablet non è consentito per ricevere/effettuare chiamate personali, SMS o altro tipo di messaggistica, giocare, durante l'orario di lavoro.
- In ogni caso si deve evitare di essere raggiunti da qualsiasi notifica o segnalazione, eventi particolarmente distraenti e disturbanti se stessi e gli altri durante lo svolgimento del proprio lavoro.
- Il personale è tenuto a mantenere i propri device silenziati durante lo svolgimento delle attività lavorative.

Caso 2
Utilizzo di funzioni che possono avere rilevanza in ambito della propria professione

- L'uso di smartphone, tablet e altri dispositivi mobili è consentito con esclusiva finalità professionale e solo in caso di necessità particolari da leggersi come: evacuazione dell'Istituto, emergenze.
- Per lavorare con strumenti di cloud computing (come GA4E/Nuvola) o più in generale se si ha necessità di essere collegati alla rete Internet a fini lavorativi *dovrà essere usata preferibilmente la connessione dell'Istituto* anche se si è dotati di accredito personale di navigazione, secondo le indicazioni date nei paragrafi precedenti.

Qualsiasi altro uso è vietato e può far incorrere in sanzioni disciplinari e pecuniarie o in veri e propri reati.

5. Prevenzione, rilevazione e gestione dei casi

Prevenzione

[39] ibidem.

Rischi	Azioni	Tempi di messa in sicurezza ragionevoli
Accesso a contenuti inopportuni di qualsiasi genere attraverso motori di ricerca via Internet e postazioni fisse di proprietà IC	*Filtraggio via server distinguendo nelle sedi della primaria e secondaria:* • Insegnanti • Alunni	*in tutti i plessi entro tre anni (fine 2019)*
Accesso a contenuti inopportuni di qualsiasi genere attraverso accesso al WiFi dell'Istituto con mobile device di Istituto o device personali autorizzati	Account personali di accesso permanenti o temporanei differenziati per: • alunni • insegnanti • visitatori	*in sede IC entro fine 2017* *in San Gerardo e Beregazzo con Figliaro entro fine 2017* *nelle altre sedi si concorderà un tempo congruo, adesso non ipotizzabile*
Smarrimento password personale o di sospetto furto identità per accrediti di istituto (sito, GS4E, registro elettronico)	Formazione continua al mantenimento in sicurezza del proprio account; Immediata informazione all'amministratore delle reti della scuola. Blocco utenza Resettaggio o cancellazione/rinnovo dell'utenza interessata	Al bisogno, il più velocemente possibile
sia come soggetto di ... sia come oggetto/vittima di... Uso non positivo e non adeguato delle TIC intese nel più largo senso possibile	Formazione continua attraverso laboratori o conferenze rivolti a tutte le componenti della comunità scolastica	Ogni anno, secondo calendario strutturato a giugno e confermato a settembre prima dell'inizio delle attività didattiche in collegio docenti e notificato in consiglio di Istituto
	Monitoraggio di comportamenti suscettibili di attenzione secondo le indicazioni date da Generazioni connesse.	Docente tiene un diario degli eventi in accordo con il DS che valuta anche sentendo il coordinatore e-safety eventuali denunce agli

	Condivisione tra tutti i membri della comunità di situazioni a rischio. Denuncia alle autorità governative di competenza. Segnalazione alla psicopedagogista, responsabile sportello ascolto della Scuola per consulto e accompagnamento nelle azioni.	organi governativi di competenza
Uso non consentito dei dispositivi fissi e mobile di proprietà della scuola scuola o personali	Formazione continua rivolta a tutte le componenti della comunità scolastica	Questo ambito sarà ciclico e continuo. Non si può definire una messa in sicurezza definitiva in ambito di assunzione di comportamenti responsabili e sicuri

Rilevazione e gestione

Che cosa segnalare	**Come segnalare: quali strumenti e a chi.**	**Come gestire le segnalazioni. Tempi di massima di presa in carico**
Navigazione in siti inadeguati. Documenti inadeguati lasciati su pc e/o condivisi. Acquisizione e/o uso di immagini, registrazioni video e audio, documenti in modo non congruo alla policy	***In caso di minore:*** registrazione sul registro di classe (elettronico e cartaceo con comunicazione alla famiglia). ***Per tutti:*** Di persona o via comunicazione telefonica: al Coordinatore della sicurezza e contestualmente al Dirigente Scolastico/vicario. In ogni caso il D.S. deve essere messo	Ogni segnalazione verrà valutata da DS e dal coordinatore sicurezza online che attiveranno a seconda della gravità dei fatti e rispetto alle evidenze, sicuramente entro una settimana dal fatto, le procedure di sanzione (compreso quelle di competenza degli organi collegiali) e se necessario gli enti governativi competenti con relativo verbale di accompagnamento.

	tempestivamente al corrente. In caso di situazione particolarmente grave verrà richiesta contestuale verbalizzazione scritta da parte del dichiarante.	
Discussioni via mail, social o chat istantanee che influiscono in modo negativo sui comportamenti assunti o usate in modo difforme da questa policy (anche casi di abusi, cybrbulismo, bullismo ecc..)	***Per tutti:*** Di persona o via comunicazione telefonica: al Coordinatore della sicurezza e contestualmente al Dirigente Scolastico/vicario. In ogni caso il D.S. deve essere messo tempestivamente al corrente. In caso di situazione particolarmente grave verrà richiesta contestualmente verbalizzazione scritta da parte del dichiarante e se si tratta di minore ci sarà il coinvolgimento immediato dei genitori.	Ogni segnalazione verrà valutata da DS e coordinatore sicurezza online che attiveranno a seconda della gravità dei fatti e rispetto alle evidenze ma sicuramente entro una settimana dal fatto, le procedure di sanzione/accompagnamento (comprese quelle di competenza degli organi collegiali) e se necessario gli enti governativi competenti con relativo verbale di accompagnamento.
In ogni situazione di sofferenza o disagio legato anche al mondo delle TIC è possibile: • riferire direttamente agli insegnanti o al team per la sicurezza online. Questi, dopo consultazione del Dirigente Scolastico, indirizzeranno l'alunno insieme alla famiglia verso i passi da compiere, rispetto alla gravità della situazione e se necessario metteranno in atto azioni di monitoraggio e accompagnamento. • usufruire dello *Sportello Ascolto* attivo nel nostro Istituto. Esso è luogo di ascolto *neutro* e *riservato*. La psicopedagogista, valuterà secondo etica professionale, i singoli casi e come procedere. È invitata tuttavia a condividere con i referenti istituzionali nei limiti di rispetto del segreto professionale informazioni e azioni volte alla tutela e al benessere dei minori.		

Questa e-safety policy con i suoi apparati è stata formulata in collaborazione con rappresentanti dei docenti, rappresentanti genitori, un gruppo di alunni della scuola secondaria, Dirigente scolastico, Dirigente servizi generali amministrativi.

Essa dovrà essere letta approvata in tutte le parti (policy e suoi apparati) in sede di Collegio docenti e Consiglio di Istituto per essere effettivamente vigente. Essa andrà ad integrare il Regolamento di Istituto - Norme Generali di Comportamento per la parte di competenza.

Olgiate Comasco, 23 novembre 2016

in fede
prof. Cosimo Capogrosso
Dirigente scolastico I.C. Olgiate Comasco

La firma autografa è omessa ai sensi dell'art. 3, c.2, D.Lgs. 39/1993

Coordinatore responsabile della proposta e stesura della e-policy
Franca Vitelli
vitelli.franca@icocscuole.it