Istituto Comprensivo di Azeglio
via XX settembre 33 - 10010 Azeglio (TO) - tel. 012572125 - 0125687523 - fax: 0125727752
Codice meccanografico: TOIC894006
E-mail istituzionale: toic894006@istruzione.it - E-mail pec: toic894006@pec.istruzione.it

2018

E-Safety Policy

DOCUMENTO PROGRAMMATICO PER FACILITARE L'UTILIZZO POSITIVO DELLE TIC E PER LA PREVENZIONE E GESTIONE DELLE SITUAZIONI PROBLEMATICHE RELATIVE ALL'USO DELLE TECNOLOGIE DIGITALI

VERSIONE 1 – AGGIORNAMENTO APRILE 2018

Generazioni Connesse
SAFER INTERNET CENTRE

Istituto Comprensivo di Azeglio

E-Safety Policy

1 Introduzione

Sia a livello internazionale, sia nel contesto italiano, la presenza sempre più diffusa delle tecnologie digitali nella vita quotidiana delle nuove generazioni apre a molte opportunità, ma pone nuove attenzioni dal punto di vista del loro uso sicuro, consapevole e positivo.
La scuola, in virtù del gravoso compito di educare, non può negare tale evidenza e non può sottrarsi dal farsi carico della responsabilità pedagogica nei confronti dei propri alunni.
L'insegnamento, l'apprendimento e il consolidamento delle competenze digitali sono un obiettivo stabilito dal Piano Nazionale Scuola Digitali (DM. N.851/2015). Secondo questo indirizzo ciò permetterebbe agli alunni, futuri cittadini, l'uso proficuo, consapevole e responsabile della tecnologia, e al contempo un'evoluzione positiva della dinamica insegnamento/apprendimento sempre più contestualizzata all'ambito del reale.

E-Safer Policy è 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 dell'Istituto Comprensivo, e tiene in debita considerazione quanto previsto dal Piano di Azione.
La Policy è un documento programmatico che impegnerà l'Istituto Comprensivo di Azeglio anche per gli anni futuri. Da ciò ne consegue che quanto descritto nel seguito verrà realizzato nel corso del prossimo triennio. Durante tale periodo, verranno monitorati gli esiti rispetto alle attese prefissate, e, in ragione dei risultati ottenuti in itinere, il presente documento sarà oggetto di ampliamento e modifica, tenendo anche in considerazione gli sviluppi contestuali e le indicazioni fornite dalle agenzie preposte.

1.1 Il contesto e termini d'uso delle TIC

1.1.1 Aree di rischio

L'Istituto Comprensivo di Azeglio, nell'elaborare il Piano di Azione, ha eseguito una valutazione dei rischi a cui possono essere esposti i propri alunni considerando la particolare fascia di età di questi ultimi.
Nello specifico, il gruppo di lavoro, tenendo conto delle indicazioni fornite dagli organi di Polizia e dalle Istituzioni che collaborano alla prevenzione del fenomeno del bullismo, cyberbullismo e affini, ha individuato tre aree di rischio:

Area di rischio	Tipologie di rischio
Contenuti	Esposizione a contenuti dannosi e non appropriati
	Siti web che promuovono stili di vita e comportamenti dannosi
	Contenuti che spingono all'odio
	Contenuti mendaci
	Pornografia
Contatto	Grooming (adescamento online), sfruttamento sessuale
	Cyberbullismo e bullismo in tutte le forme
	Furto di identità
	Pedopornografia
Condotta	Comportamenti aggressivi
	Violazione della privacy e divulgazione di dati personali
	Reputazione digitale
	Dipendenza da Internet
	Eccesso d'uso dei videogiochi online
	Sexting
	Violazione del copyright

1.1.2 Uso delle TIC a scuola

All'interno dell'Istituto Comprensivo di Azeglio è ammesso solo l'uso di strumenti informatici (mobile e fissi) in modalità cablata e/o WiFi di proprietà dello stesso Istituto Comprensivo.

Nel caso specifico del personale docente e ATA, è loro permesso l'impiego di dispositivi propri (smartphone, tablet, notebook) purché finalizzato allo svolgimento delle attività scolastiche (didattiche, organizzative, ecc).

È altresì ammesso l'uso dei dispostivi personali ai fornitori esterni e al personale che svolge attività di supporto alla didattica (es. educatori) per l'assolvimento dei compiti assegnati e limitatamente allo svolgimento di tali attività.

Agli alunni è sempre fatto divieto d'usare i dispositivi propri (connessi e non connessi) entro le aree comuni esterne ed interne del plesso scolastico, le aule e i laboratori.

1.2 Scopo e destinatari della Policy

1.2.1 Scopo della Policy

Il presente documento ha il duplice scopo di prevenire e gestire situazioni problematiche relative all'uso di tecnologie digitali e facilitare e promuovere l'utilizzo positivo delle TIC (Tecnologie dell'Informazione e Comunicazione) nella didattica e negli ambienti scolastici dell'Istituto Comprensivo di Azeglio. Nello specifico gli scopi del presente documento sono così riassumibili:

- definire i principi fondamentali condivisi da tutti i membri della comunità scolastica rispetto all'uso delle TIC,
- salvaguardare e proteggere i bambini, i ragazzi e tutto il personale dall'uso improprio delle TIC e dai soggetti che le utilizzano in modo deviato,
- assistere il personale della scuola nel lavorare in modo sicuro e responsabile con le TIC,
- monitorare i propri standard e le prassi,
- definire chiare aspettative di comportamento per un uso responsabile della rete Internet, sia in ambito didattico sia al di fuori di tale contesto,
- avere procedure chiare per affrontare l'uso improprio degli strumenti digitali o gli abusi online,
- assicurarsi che tutti i membri della comunità scolastica siano consapevoli che i comportamenti illeciti o pericolosi sono inaccettabili e sanzionati a norma del Regolamento di Istituto e della legislazione vigente,

1.2.2 Destinatari della Policy

La presente Policy si applica a tutta la comunità scolastica dell'Istituto Comprensivo di Azeglio. Nello specifico è rivolta:

- ai bambini, che frequentano la scuola dell'Infanzia e la scuola Primaria;
- ai ragazzi della Secondaria di Primo Grado;
- a tutto il personale docente che svolge la sua attività di insegnamento nei plessi dell'Istituto Comprensivo, anche per brevi periodi;
- al Dirigente Scolastico (DS) e al Dirigente dei Servizi Generali e Amministrativi (DSGA);
- a tutto il personale amministrativo e a tutti i collaboratori scolastici (ATA);
- a tutti gli operatori/professionisti e/o volontari che entrano a scuola;
- ai genitori e famiglie degli alunni;

- ai visitatori/ospiti;
- a tutti coloro che hanno accesso ai sistemi di connessione e usano qualsiasi strumentazione digitale della scuola o anche dispositivi personali dentro e fuori dall'Istituto Comprensivo.

1.3 Ruoli e responsabilità

Il referente d'Istituto per la prevenzione al bullismo e cyberbullismo (più avanti solo Referente d'Istituto – nominato secondo le disposizioni della L. 107/2017), in collaborazione con l'Animatore Digitale, assistiti dal Team per l'innovazione tecnologica, hanno la funzione di coordinare le attività descritte nella presente Policy in accordo con quanto definito nel Piano di Azione, di aggiornarla annualmente (se necessario), di presentarla al Collegio ad ogni inizio di anno scolastico e renderla pubblica attraverso gli organi di informazione di cui è dotata la scuola (es. sito web istituzionale) e durante gli incontri e i momenti di incontro con gli alunni in ingresso.

Le due figure succitate hanno altresì la funzione di monitorare l'applicazione della Policy da parte dei colleghi docenti e del personale ATA riferendo eventuali problemi al Dirigente Scolastico, mentre ciascun insegnante ha la responsabilità di monitorarne l'applicazione da parte dei propri studenti.

È in capo al Referente d'Istituto, sentito l'Animatore Digitale, il Team Digitale e gli altri organi collegiali preposti e il Gruppo di Lavoro per l'Inclusività (GLI), proporre e incentivare le attività di formazione e informazione per gli alunni che hanno come obiettivo la prevenzione dei casi di bullismo, cyberbullismo, sexting, violazione della privacy, adescamento, pedopornografia.

La rilevazione dei casi avviene durante la normale attività dei docenti curricolari, del Referente d'Istituto, dell'Animatore Digitale, dello sportello di ascolto e del personale ATA in servizio presso la scuola, degli educatori esterni in servizio presso il plesso, e più in generale di tutto il personale professionale che svolge un'attività continuativa e inquadrata nell'organigramma scolastico (es. psicologo dello sportello di ascolto).

In caso di segnalazione, il personale scolastico (docente, ATA, educatori, ecc.) avrà come primo interlocutore il Referente d'Istituto, il quale informerà tempestivamente il Dirigente Scolastico (o in sua assenza/impossibilità il Vicario) dell'accaduto.

Nello specifico si evidenziano nel seguito le responsabilità chiave per i principali soggetti coinvolti nell'applicazione delle Policy.

Ruolo	Responsabilità
Dirigente Scolastico e DSGA	➢ 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 della gestione dei dati e della sicurezza delle informazioni e garantisce l'utilizzo delle corrette procedure di trattamento dei dati personali; ➢ 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.
Team Digitale	➢ si fanno carico giorno per giorno 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; ➢ garantiscono che tutto il personale sia a conoscenza delle procedure che devono essere seguite in caso di incidente di sicurezza on-line; ➢ collaborano, in base alle necessità, con il personale tecnico esterno per il raggiungimento degli obiettivi di sicurezza previsti dalla Policy.
Referente d'Istituto per il bullismo e cyberbullismo	
Animatore Digitale	➢ 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 Dirigente Scolastico.

Ruolo	Responsabilità
Docente Responsabile di Laboratorio **Docente del pronto soccorso tecnologico**	➢ segnalano problemi relativi alla sicurezza online rilevati al DS e al Referente d'Istituto per il bullismo e cyberbullismo; ➢ gestiscono 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 siano attivi; • presso il plesso sia attivo e funzionale il sistema di web filtering. ➢ si tengono aggiornati sulla policy di sicurezza online della scuola e condividono le informazioni tecniche al fine di svolgere efficacemente il proprio ruolo.
Insegnanti	➢ leggono, approvano in sede collegiale e aderiscono alla presente Policy di utilizzo; ➢ educano alla sicurezza online nello svolgersi del 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). ➢ segnalano al Referente d'Istituto (oppure al docente responsabile del laboratorio, oppure ad un membro del Team Digitale, oppure al fiduciario del plesso scolastico) qualsiasi abuso sospetto o accertato.
Tutto il personale dell'Istituto, gli educatori, gli esperti esterni e i volontari	➢ devono leggere, comprendere, aderire alla presente Policy; ➢ devono segnalare qualsiasi abuso sospetto o qualsiasi problema al Referente d'Istituto (o in alternativa al docente responsabile del laboratorio, oppure ad un membro del Team Digitale, oppure al fiduciario del plesso scolastico); ➢ 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.

Ruolo	Responsabilità
Bambini e ragazzi	➢ leggono, capiscono, e aderiscono alla presente Policy; ➢ 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.
Genitori	➢ leggono, capiscono, e aderiscono alla presente Policy; ➢ si consultano con il Referente d'Istituto, il Fiduciario di plesso e il Dirigente Scolastico se hanno preoccupazioni circa l'uso della tecnologia online o offline da parte dei loro figli; ➢ sostengono la scuola nel promuovere la sicurezza online.

1.3.1 Integrazione e diffusione e comunicazione della Policy

La Policy fa riferimento e si armonizza con tutti gli altri regolamenti vigenti nell'Istituto Comprensivo in particolare con il Regolamento di Istituto. Tutto ciò che qui non è normato è da considerarsi regolamentato secondo tale disciplina generale.

La Policy verrà comunicata alla comunità scolastica e alle persone che usufruiscono dei servizi scolastici nei seguenti modi:

- sul sito dell'Istituto Comprensivo una volta approvata in modo definitivo;
- nelle bacheche degli spazi pubblici dei plessi.

La Policy diventa parte integrante delle norme e dei regolamenti che l'Istituto Comprensivo autodefinisce nell'ambito dell'autonomia scolastica.

All'atto della nuova iscrizione o inserimento nel posto di lavoro, i contenuti della Policy verranno comunicati alla famiglia dell'alunno e al dipendente diventando oggetto di accettazione obbligatoria.

1.4 Gestione delle infrazioni alla Policy

L'Istituto Comprensivo di Azeglio prenderà e manterrà nel tempo tutte le precauzioni necessarie per garantire agli alunni e al personale l'accesso ai soli contenuti digitali. Tuttavia, va precisato che dati i limiti umani e tecnologici, è di fatto impossibile per l'Istituto Comprensivo evitare in assoluto che gli alunni, durante le attività scolastiche che necessitano dell'uso delle TIC, possano imbattersi in contenuti inappropriati.

In questo senso, l'Istituto Comprensivo non può farsi carico della responsabilità per il materiale trovato su internet o per eventuali conseguenze causate dall'accesso ad internet.

Qualora dovesse accadere un incidente, il Referente d'Istituto è la figura interna alla scuola che deve essere informata e allertata contestualmente al Fiduciario del plesso.

Qualsiasi sospetto, rischio, violazione evidenziati sulla popolazione studentesca vanno segnalati in giornata al Referente d'Istituto che a sua volta riferirà al Dirigente Scolastico. Qualsiasi allerta di uso improprio delle TIC, riferito al personale che a vario titolo presta servizio all'interno degli edifici scolastici, va sempre riferito direttamente al Dirigente Scolastico.

In caso di infrazione alla Policy, il personale, gli alunni e gli altri componenti della comunità scolastica interessati verranno prontamente informati attraverso formale notifica del DS o del Vicario, o del Fiduciario del plesso scolastico. Contestualmente verranno notificate le eventuali sanzioni,

Conformemente a quanto indicato nel Regolamento di Istituto, le sanzioni comminate agli alunni avranno carattere educativo/riabilitativo e in ogni caso verrà coinvolta la famiglia, in qualità di primi educatori.

Le infrazioni compiute dagli alunni e considerate "di lieve entità" (secondo il giudizio del personale scolastico competente) verranno gestite dal Coordinatore della Classe unitamente al Fiduciario del plesso scolastico in rapporto con il Referente d'Istituto. Tali infrazioni verranno sanzionate come previsto dal Regolamento di Istituto.

1.5 Monitoraggio dell'efficacia e aggiornamento della Policy

La Policy sarà oggetto di riesame con cadenza annuale e/o al verificarsi di cambiamenti significativi per quanto riguarda le tecnologie in uso all'interno della scuola e/o il recepimento delle nuove disposizioni normative nazionali.

Il gruppo di riesame e aggiornamento è composto dal Dirigente Scolastico, dal Team Digitale, dal Referente d'Istituto.

2 Formazione e Curricolo

2.1 Formazione degli alunni

Il curricolo verticale relativo alle competenze digitali è in corso di definizione puntuale. In linea generale sarà orientato al raggiungimento dei due obiettivi fondamentali:

- apprendere l'uso attento e responsabile delle TIC;
- responsabilizzare gli studenti davanti alla scelta dei comportamenti da assumere durante l'utilizzo delle TIC nei vari contesti d'impiego;

Per il raggiungimento di tali obiettivi, l'Istituto Comprensivo si avvarrà in modo strutturale delle risorse strumentali e professionali messe in campo dalla rete di ambito, dagli Enti e Istituzioni presenti sul territorio, secondo quanto indicato nel Piano di Azione.

2.2 Formazione dei docenti e del personale ATA

Al fine di rendere i propri docenti formati e informati sui temi all'oggetto della presente Policy, l'Istituto Comprensivo di Azeglio attiva una campagna informativa di sensibilizzazione per la partecipazione alle iniziative organizzate dall'Ufficio Scolastico Regionale, da altri enti e associazioni territoriali (es. Associazione Gessetti Colorati).

Parallelamente a ciò, l'Istituto Comprensivo ha promosso la partecipazione dei docenti ai corsi di formazione nell'ambito della rete di scopo TO08, aventi per oggetto il potenziamento della competenza digitale.

È compito del Team digitale analizzare in modo mirato il fabbisogno formativo dei colleghi docenti in materia di TIC, avviando specifici percorsi formativi aggiuntivi, distribuendo e condividendo il materiale informativo. A tal fine, verrà attivata un'apposita area del sito web istituzionale in cui rendere accessibili i documenti.

Indipendentemente dalla partecipazione alle iniziative di formazione, resta sempre attiva la disponibilità dell'Animatore Digitale, del Team Digitale e del Referente d'Istituto a fornire suggerimenti e consigli in materia di TIC e didattica.

Per la sensibilizzazione e formazione del personale ATA, soprattutto coloro che lavorano a stretto contatto con gli alunni, l'Istituto Comprensivo promuove la partecipazione dei dipendenti agli incontri e seminari organizzati dagli Enti e Uffici competenti.

2.3 Sensibilizzazione delle famiglie.

A seguito della compilazione del Piano di Azione, l'Istituto Comprensivo si è attivato per sollecitare la partecipazione delle famiglie agli eventi di formazione e ai seminari organizzati dall'Ufficio Scolastico Regionale. Gli inviti sono stati estesi per mezzo di comunicazioni mirate.

È intenzione dell'Istituto Comprensivo continuare a informare le famiglie degli alunni circa i tempi e le modalità di svolgimento cercando di suscitare interesse. In contemporanea, l'Istituto cercherà, compatibilmente con le risorse finanziare disponibili, di organizzare al proprio interno momenti di condivisione e confronto con le famiglie sui temi all'oggetto della presente Policy. Tali interventi verranno prontamente promossi attraverso i canali informativi di Istituto.

3 Gestione dell'infrastruttura e della strumentazione ICT

L'Istituto Comprensivo gestisce linee internet dedicate esclusivamente alla didattica (in tutte le sedi) e una linea esclusiva per la parte amministrativa (sede centrale).

Lo stesso accade per gli ambienti online: il sito istituzionale è distinto dall'ambiente online di apprendimento (Google Classroom).

Il sito istituzionale viene integrato da due ambienti digitali, i cui dati sono di proprietà dell'Istituto Comprensivo, ma sono manutenuti e ne viene garantita la sicurezza da terzi: il registro digitale (Gruppo Spaggiari Parma) e la segreteria digitale (Regel).

3.1 Infrastruttura e strumentazione ICT

All'interno dell'Istituto Comprensivo le nuove tecnologie sono utilizzate prevalentemente:

- nei laboratori di informatica;
- nelle aule dotate di LIM;
- nelle sale docenti;
- negli uffici di segreteria.

I plessi scolastici sono dotati di connessione internet cablata e/o WiFi protetta con WPA2. Nei plessi con il maggior numero di classi, la rete cablata/WiFi è dotata di apposito firewall per il filtraggio e monitoraggio del traffico dati interno.

Secondo quanto previsto dal Piano di Azione, è obiettivo dell'Istituto Comprensivo, compatibilmente con i fondi economici disponibili, dotare tutti i plessi di un proprio sistema di filtraggio avanzato.

Attualmente la maggior parte dei PC (desktop e notebook) sono protetti da antivirus regolarmente aggiornati e gli alunni hanno accesso alla navigazione soltanto in presenza del loro docente. È intenzione dell'Istituto Comprensivo estendere la protezione locale a tutti i PC.

3.1.1 Accesso alla rete e ai servizi on line di Istituto

Per garantire che la rete e i servizi on line d'Istituto vengano utilizzati in modo sicuro, l'Istituto Comprensivo:

- garantisce che l'accesso alle TIC e alla rete avvenga solo ed esclusivamente in presenza di un docente o di personale qualificato della scuola;

- garantisce l'accesso ai servizi online attraverso username unici e password (registro elettronico, Google Classroom, Regel). L'utente (docente e studente) si impegna a non cedere a nessuno le proprie credenziali/password;
- 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;
- 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;
- garantisce l'utilizzo del 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);

3.1.2 Gestione delle password

Preso atto della criticità della password personale di accesso ai servizi online, l'Istituto Comprensivo 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 agli uffici di segreteria, che provvederanno ad una sua sostituzione;

- tutto il personale e gli alunni hanno il proprio nome utente e password univoci privati per accedere ai sistemi scolastici (registro elettronico, segreteria digitale, ecc);
- tutti gli utenti (docenti e studenti) hanno la responsabilità di mantenere la(e) propria password(s) privata(e);
- la password personale 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.

3.2 Ambienti digitali on line di Istituto

3.2.1 Sito web Istituzionale

Il sito web istituzionale è gestito da un docente referente con incarico effettivo. I genitori, all'atto dell'iscrizione, esprimono o meno il proprio consenso all'utilizzo di foto e notizie relative agli alunni per l'aggiornamento del sito.

Quando viene pubblicato o linkato il lavoro di altri, il docente referente indica chiaramente gli accrediti alle fonti utilizzate e l'identità o lo stato dell'autore. L'Istituto Comprensivo garantisce che le fotografie pubblicate sul web non verranno mai nominate con nomi completi dei soggetti né avranno didascalie così composte. Non verranno indicati i nomi degli alunni quando verranno salvati file, immagini o tag nella pubblicazione sugli spazi web della scuola.

3.2.2 Registro elettronico, segreteria digitale e ambienti di apprendimento on line

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 scolastico e di segreteria in base alle loro competenze: ad esempio tutti gli insegnanti di classe possono caricare informazioni nelle loro aree di pertinenza. Per queste procedure si utilizza il protocollo di navigazione https.

Fotografie e video aventi per soggetto alunni, famiglie e personale scolastico, potranno essere pubblicati solo ed esclusivamente sul sito web istituzionale dal docente referente.

A scuola, gli studenti possono caricare e pubblicare esclusivamente all'interno del sistema Google Classroom.

3.3 Uso privato di spazi on line da parte del personale scolastico

Nel normale uso di spazi online personali (social network, blog, siti web, ecc), il personale scolastico in servizio presso l'Istituto Comprensivo di Azeglio, deve attenersi scrupolosamente alle seguenti norme che vanno ad impattare sulla vita scolastica:

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

3.4 Protezione dei dati personali

3.4.1 Pratiche strategiche e operative

Presso l'Istituto Comprensivo di Azeglio sono in uso le seguenti pratiche atte a proteggere i dati personali:

- il responsabile del trattamento dei dati personali dell'Istituzione scolastica è il Dirigente Scolastico;
- il Dirigente Scolastico designa quali incaricati sono preposti al trattamento dei dati definendo i criteri di gestione;
- il personale incaricato è istruito sulla procedura da seguire per segnalare eventuali incidenti dove la protezione dei dati potrebbe essere stata compromessa.

3.4.2 Soluzioni tecniche adottate

Il personale incaricato della gestione dei dati personali ha un'area protetta sulla rete per memorizzare i file sensibili (segreteria digitale e registro elettronico). Al personale autorizzato viene richiesto di usare i sistemi di logout al momento di lasciare la postazione usata.

Gli uffici di segreteria sono dotati di mezzi elettronici adeguati ad impedire l'accesso dall'esterno alla rete, quali firewall od altri strumenti.

4 Strumentazione personale

4.1 Note generali

Il personale scolastico, gli esperti di progetto, gli educatori, i volontari, gli alunni e i genitori o i visitatori che portano all'interno dei plessi scolastici dell'Istituto i dispositivi mobili di loro proprietà ne sono direttamente responsabili: la scuola non risponde direttamente/indirettamente di guasti, smarrimenti, perdita di dati, malfunzionamenti. Va ricordato che i dispositivi mobili personali non possono essere utilizzati in alcune aree interne o di pertinenza dell'Istituto.

Nell'esercizio delle funzioni di sorveglianza e tutela, il Dirigente Scolastico ha la possibilità di richiedere la verifica ispettiva dei dispositivi personali in caso di ragionevole sospetto che possano contenere materiale illegale o indesiderabile (es. pornografia, violenza o bullismo, registrazioni di qualsiasi genere vietate, ecc.…). L'ispezione verrà eseguita secondo le norme vigenti dagli organi di polizia preposti.

4.2 Acquisizione di immagini e video digitali

Presso l'Istituto Comprensivo di Azeglio:

- viene chiesto esplicito permesso dei genitori/tutore legale per utilizzare fotografie digitali o video che coinvolgono il loro figlio. L'autorizzazione viene sottoscritta all'iscrizione, o annualmente all'inizio delle attività didattiche;
- non vengono identificati gli alunni all'interno di materiali fotografici online o distribuiti su supporti offline;
- accettando e sottoscrivendo questa policy, i docenti dell'Istituto si impegnano secondo le clausole dette nell'uso dei dispositivi mobili personali per scattare foto/fare dei video ad alunni.

Si rammenta 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.

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 Comprensivo e di documentazione pedagogica.

La diffusione di contenuti è permessa solo sui canali ufficiali di proprietà dell'Istituto Comprensivo, in ogni caso è sempre subordinata all'autorizzazione del Dirigente Scolastico.

Si richiama l'attenzione di 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.

4.3 Norme d'uso dei dispositivi – Studenti

L'Istituto Comprensivo consiglia vivamente a tutti gli studenti di non portare telefoni cellulari e dispositivi mobili personali a scuola. Qualora l'alunno decida di portare con sé il telefono o altro dispositivo mobile, lo fa sotto la sua diretta responsabilità. La scuola non può essere considerata responsabile per manomissioni, furti, danneggiamenti. Sarà cura dell'alunno conservare in un luogo sicuro il dispositivo.

L'uso dei dispositivi personali (telefono, tablet, ecc) è assolutamente vietato in ogni ambiente interno ed esterno di pertinenza della scuola e in ogni contesto didattico/educativo (lezioni, intervalli, pausa mensa, uscite didattiche, ecc). Il dispositivo deve essere tassativamente tenuto spento durante le attività didattiche, educative e ricreative che si svolgono sotto la supervisione e il controllo del personale scolastico (docente, ATA, educatori, ecc).

L'estensione del divieto ai momenti di permanenza a scuola come l'intervallo, la pausa mensa, il cambio dell'ora, ecc., oltre a rispondere a necessità organizzative e di controllo, ha una motivazione educativa. L'Istituto Comprensivo ritiene importante valorizzare momenti di relazione positiva tra gli studenti, evitando atteggiamenti di esclusione, di isolamento e di separazione dalla vita scolastica reale.

In caso di necessità ed emergenze, sarò cura del personale scolastico contattare le famiglie per conto dell'alunno, o, viceversa, lo studente per conto dei famigliari, attraverso i canali ufficiali della scuola (telefono del plesso scolastico, mail istituzionale).

Se un alunno viola questa Policy, il dispositivo verrà immediatamente confiscato dal personale in servizio, il quale lo deporrà in un luogo sicuro in ufficio di segreteria. Contestualmente verrà data comunicazione ai genitori in forma scritta/orale attraverso i canali ufficiali scuola-famiglia (telefono, diario, registro elettronico).

La restituzione dei dispositivi sequestrati verrà effettuata secondo le modalità previste dal Regolamento di Istituto, comunque durante un incontro tra docente e famiglia in cui, se necessario, verrà notificata l'eventuale sanzione disciplinare.

Telefoni e dispositivi personali non possono essere mai usati durante gli esami o le prove nazionali.

4.4 Norme d'uso dei dispositivi – Personale scolastico

Il personale che svolge la propria mansione all'interno degli ambienti scolastici (docenti, ATA, educatori, volontari, specialisti, ecc) 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.

Per ragioni di privacy e sicurezza, la comunicazione Bluetooth dovrebbe essere impostata in modalità nascosta o spenta.

Il personale scolastico (docenti, ATA, educatori, volontari, ecc) in servizio è tenuto a mantenere i propri dispositivi spenti, fatta eccezione se utilizzati per lo svolgimento dell'attività didattica (es. completamento del registro elettronico).

In ogni caso il personale in servizio deve evitare di essere raggiunto da qualsiasi notifica o segnalazione o eventi particolarmente distraenti e disturbanti la stessa attività didattica.

I cellulari non dovranno essere utilizzati durante l'insegnamento e/o l'attività didattica ed educativa, a meno che non sia stato concesso un permesso esplicito dal Dirigente Scolastico. Al ricevimento dell'autorizzazione, il docente chiarirà prontamente ai propri studenti l'eccezionalità della situazione dichiarando di aver ricevuto specifica autorizzazione dal Dirigente.

Il divieto si applica anche negli intervalli e in altre situazioni che sono assimilabili ad attività didattica/educativa come mensa, cambio dell'ora, intervalli.

In linea di principio, il personale scolastico (docenti, ATA, educatori, volontari, ecc) non deve utilizzare dispositivi di proprietà personale, come cellulari o macchine fotografiche, per scattare foto, video, registrazioni audio/video che coinvolgano gli alunni, e preferenzialmente utilizzare solo le attrezzature adatte allo scopo di proprietà della scuola.

Se la scuola non possedesse tali attrezzature, potrà utilizzare le proprie previo permesso del Dirigente Scolastico, e seguire le norme illustrare nel presente documento.

In caso di necessità si può 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 dati sensibili o personali. Dovrà comunque riferire l'incidente al Dirigente Scolastico.

Il personale della scuola ha facoltà di utilizzo del proprio telefono cellulare durante i periodi di pausa, seguendo le regole generali di non disturbo delle attività.

Le infrazioni a queste norme, possono comportare il richiamo formale da parte del Dirigente Scolastico, e altre sanzioni ritenute necessarie in funzione alla gravità della situazione.

5 Prevenzione, rilevazione e gestione dei casi

Qualsiasi situazione sospetta è meritevole di rilevazione. I possibili rischi per gli alunni possono essere così sintetizzati:

- uso improprio di internet;
- cyberbullismo;
- sexting;
- adescamento;
- violazione della privacy (immagini);
- istigazione alla violenza e all'autolesionismo.

I segnali sociali che possono insospettire il personale scolastico (docente, ATA, educatore, ecc) vanno dal chiacchierio prolungato in classe dopo i momenti ricreativi, ai cambiamenti improvvisi nel modo di porsi con i pari. Dal calo nel rendimento scolastico apparentemente immotivato all'isolamento volontario dal gruppo. Ovviamente questi costituiscono solo un elenco indicativo e non esaustivo.

Va ricordato che il docente, l'educatore, e più in generale il personale in servizio presso una scuola deve farsi guidare dal principio del "superiore interesse del minore". La priorità non è trovare il responsabile. Nell'immediato occorre evitare indagini e limitarsi e registrare quanto accaduto.

5.1 Prevenzione dei casi in base al rischio

Rischio	Azioni	Tempi di esecuzione
Accesso a contenuti inopportuni di qualsiasi genere attraverso motori di ricerca via Internet e postazioni fisse di proprietà dell'Istituto	Filtraggio selettivo mediante apparecchiature hardware	In base alla disponibilità economica
Accesso a contenuti inopportuni di qualsiasi genere attraverso accesso al WiFi dell'Istituto con mobile device di Istituto o device personali autorizzati	Filtraggio selettivo mediante apparecchiature hardware.	In base alla disponibilità economica
Smarrimento password personale o di sospetto furto	Formazione continua al mantenimento in sicurezza del proprio account;	Durante le attività didattiche curricolari/extracurricolari

Rischio	Azioni	Tempi di esecuzione
d'identità per servizi on line di Istituto	Immediata informazione degli uffici di segreteria	Contestuale alla rilevazione del problema
	Blocco utenza. Reset o cancellazione/rinnovo dell'utenza interessata	Entro 24 ore dalla segnalazione/in base ai tempi tecnici della piattaforma in uso
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	Durante l'anno scolastico
	Monitoraggio di comportamenti suscettibili di attenzione secondo le indicazioni date da "Generazioni connesse".	Contestualmente agli eventi, il Referente di Istituto per il bullismo e il cyberbullismo mantiene attivo un registro delle segnalazioni in cui si annotano i casi e le contromisure attivate (vedi allegato alla Policy). Il DS valuta celermente eventuali denunce agli organi governativi di competenza.
	Condivisione tra tutti i membri della comunità scolastica interessati. Eventuale denuncia alle autorità governative di competenza. Segnalazione alla psicopedagogista, responsabile dello sportello di ascolto della Scuola per consulto e accompagnamento nelle azioni.	Celermente, in base alla disponibilità del Consiglio di Classe o Interclasse. In base alla disponibilità delle figure professionali esterne.
Uso non consentito dei dispositivi fissi e mobili di proprietà della scuola o personali	Formazione continua rivolta a tutte le componenti della comunità scolastica. Sequestro immediato dello strumento personale. Attivazione contestuale delle procedure di segnalazione alla famiglia.	La formazione avverrà durante il normale anno scolastico. Gli interventi correttivi e di segnalazione sono contestuali all'evento.

5.2 Rilevazione e gestione dei casi

Cosa segnalare	Come segnalare	Come gestire
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 con comunicazione alla famiglia **Per tutti:** Immediata comunicazione orale: al Referente di Istituto e contestualmente al Dirigente Scolastico/Vicario e Fiduciario di plesso. Compilazione della scheda di segnalazione da inoltrare alla segreteria (vedi allegato) Nei casi di particolare gravità è richiesta la verbalizzazione da parte del personale interessato da allegare al registro del Referente d'Istituto	Ogni segnalazione verrà valutata dal DS e dal Referente d'Istituto per il bullismo e il cyberbullismo che attiveranno celermente, a seconda della gravità dei fatti e rispetto alle evidenze, le procedure di sanzione (compreso quelle di competenza degli organi collegiali) e se necessario gli enti governativi competenti con relativo verbale di accompagnamento.
Discussioni via mail, social o chat istantanee che influiscono in modo negativo sui comportamenti assunti o usate in modo difforme dalla Policy (anche casi di abusi, cyberbullismo, bullismo ecc..)	**Per tutti:** Immediata comunicazione orale al Referente di Istituto e contestualmente al Dirigente Scolastico/Vicario e Fiduciario del plesso. In ogni caso il D.S. deve essere messo tempestivamente al corrente. Compilazione della scheda di segnalazione da inoltrare alla segreteria (vedi allegato) In caso di situazione particolarmente grave, verrà richiesta contestualmente una verbalizzazione scritta da parte del dichiarante e, se si tratta di minore, ci sarà il coinvolgimento immediato dei genitori.	Ogni segnalazione verrà valutata dal DS e dal Referente d'Istituto che attiveranno celermente, a seconda della gravità dei fatti e rispetto alle evidenze, le procedure di sanzione/accompagnamento (comprese quelle di competenza degli organi collegiali) e se necessario gli enti governativi competenti con relativo verbale di accompagnamento.

Cosa segnalare	Come segnalare	Come gestire
In ogni situazione di sofferenza o disagio legato anche al mondo delle TIC è possibile: ➢ riferire direttamente agli insegnanti di classe, al Referente di Istituto. 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 nell'Istituto Comprensivo. Esso è luogo di ascolto neutro e riservato. La psicologa 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.		

SCHEDA DI SEGNALAZIONE		
Nome di chi compila la segnalazione		
Ruolo		
Data		
Ora		
Plesso		
Descrizione dell'episodio o del problema		
Soggetti coinvolti	Nomi di chi ha subito: Classe: 1. 2. 3. Nomi di chi ha agito: Classe: 1. 2. 3.	
Chi ha riferito dell'episodio?	☐ Chi ha subito ☐ Un compagno (nome): ☐ Genitore (nome): ☐ Insegnante (nome): ☐ Altri, specificare: ……..	
Atteggiamento del gruppo	Da quanti compagni è sostenuto chi ha agito? Quanti compagni supportano chi ha subito o potrebbero farlo?	
Gli insegnanti sono intervenuti? Come?		
La famiglia o altri adulti hanno cercato di intervenire?		
Chi è stato informato della situazione?	☐ coordinatore di classe/team ☐ referente ☐ dirigente scolastico ☐ la famiglia di chi ha subito ☐ la famiglia di chi ha agito ☐ le forze dell'ordine/enti preposti ☐ altro, specificare	data: data: data: data: data: data: data:

MODULO PER IL FOLLOW UP DEI CASI		
	Azioni intraprese	**La situazione è…**
Aggiornamento 1		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 2		□ migliorata □ invariata □ peggiorata Come:
Aggiornamento 3		□ migliorata □ invariata □ peggiorata Come:
Riferimento ad altri casi		□ migliorata □ invariata □ peggiorata Come:

REGISTRO DELLE SEGNALAZIONI E GESTIONE

Plesso:	**Anno Scolastico:**

Classe	**Data**	**Ora**	**Episodio (sintesi descrittiva)**	**Azioni intraprese**			**Insegnante che ha segnalato**	**Firma**
				Cosa è stato attuato	**Da chi è stato attuato**	**Esito dell'intervento**		