ISTITUTO COMPRENSIVO STATALE DI PREVALLE
Viale Rimembranze,3 -25080 Prevalle (BS) -tel. 030/603315
CF 87030820176 – COD. MECC. BSIC86700Q
bsic86700q@istruzione.it –bsic86700q@pec.istruzione.it
www.icprevalle.gov.it

Comunicazione n. 118 Prevalle , 19.11.19

Al Personale Docente e Ata
Alle Famiglie
Agli Alunni

LINEE GUIDA PER L'USO DELLE RISORSE TECNOLOGICHE DI RETE

1. Scopi di una politica d'uso accettabile e sicuro della rete della scuola

Scopo del presente documento è quello di informare l'utenza al fine di garantire un uso corretto e responsabile delle apparecchiature informatiche collegate alla rete in dotazione alla Scuola, nel rispetto della normativa vigente.
Il curricolo scolastico prevede che gli alunni imparino a trovare materiale, recuperare documenti e scambiare informazioni utilizzando le TIC (Tecnologie di Comunicazione Informatica). Internet offre sia agli alunni che agli insegnanti una vasta scelta di risorse diverse e opportunità di scambi culturali con gli studenti di altri paesi, risorse per il tempo libero, le attività scolastiche e sociali. Pertanto la Scuola promuove l'uso delle Tecnologie Informatiche e della Comunicazione (di seguito denominate "TIC") come supporto dei processi di insegnamento - apprendimento, nell'ottica di una didattica inclusiva, con opportunità e modalità diverse ai fini del successo formativo, cognitivo e psico-sociale degli alunni, per promuovere l'eccellenza in ambito didattico attraverso la condivisione delle risorse, l'innovazione e la comunicazione.
Gli utenti, siano essi maggiorenni o minori, devono essere pienamente consapevoli dei rischi a cui si espongono quando navigano in rete. Di fatto esiste la possibilità che durante il lavoro online si possa entrare accidentalmente in contatto con materiale inadeguato e/o illegale, pertanto la Scuola promuove l'adozione di strategie che limitino l'accesso a siti e/o applicazioni illeciti: è infatti dovere della Scuola garantire il diritto dei minori all'accesso alla rete e adottare nel contempo tutti i sistemi di sicurezza conosciuti per diminuire le possibilità di rischio nella navigazione.
Gli insegnanti hanno la responsabilità di guidare gli alunni nelle attività on-line, di stabilire obiettivi chiari nell'uso di Internet e insegnarne un uso accettabile e responsabile, di individuare regole di condotta chiare per un uso critico e consapevole di Internet anche a casa al fine di prevenire il verificarsi di situazioni potenzialmente pericolose.
Resta fermo che non è possibile garantire una navigazione totalmente priva di rischi e che la Scuola e gli insegnanti non possono assumersi le responsabilità conseguenti all'accesso accidentale e/o improprio a siti illeciti, o al reperimento ed uso di materiali inappropriati.
La scuola ha elaborato questo documento in conformità con le LINEE DI ORIENTAMENTO per azioni di prevenzione e di contrasto al bullismo e cyberbullismo (aprile 2015) elaborate dal Ministero dell'Istruzione, dell'Università e della Ricerca in collaborazione con il Safer Internet Center per l'Italia, programma comunitario istituito dal Parlamento Europeo e dal Consiglio dell'Unione.
Le regole approvate nel presente disciplinare tecnico devono avere una valenza formativa e non solo sanzionatoria, perché il loro scopo è quello di aiutare gli utenti meno esperti a orientarsi in merito a temi quali la privacy, la libertà di espressione, il plagio, l'identificazione ed identità di rete, l'etica nella rete, i

vincoli legali, le molestie, l'utilizzo delle risorse.

Le linee guida si propongono di perseguire le seguenti finalità:

- garantire la massima efficienza delle risorse,
- garantire la riservatezza delle informazioni e dei dati,
- provvedere ad un servizio continuativo nell'interesse della comunità scolastica,
- provvedere ad un'efficiente attività di monitoraggio,
- garantire il rispetto delle leggi in materia di utilizzo delle risorse informatiche,
- garantire la massima sicurezza nell'interazione tra l'Istituto e gli altri soggetti pubblici o privati e ottimizzare i costi di esercizio.

2. Riferimenti normativi

II presente documento è stato redatto in conformità alle seguenti disposizioni normative, per quanto attiene al settore scolastico:

- D.P.R. n. 275 del 25/02/1999, Regolamento recante norme in materia di autonomia delle istituzioni scolastiche, ai sensi dell'alt. 21 della legge 15 marzo 1997, n. 5;
- C. M. 114/2002, Sulle infrastrutture tecnologiche nelle scuole e nuove modalità di accesso al sistema informativo.
- D.lgs 196/2003 T.U. sulla privacy entrato in vigore il 1/1/2004 che riassume le norme precedenti sulla privacy;
- L. 325/2000 sull'adozione delle misure di sicurezza nel trattamento dei dati in applicazione dell'alt. 15 della L. 675/1996;
- L. 547/ 1993: norme in materia di reati informatici;
- L. 4/2004, Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici;
- Raccomandazione del Parlamento Europeo e del Consiglio del 18 /12/2006 (competenza digitale come competenza chiave)
- D. lgs 305/2006 del 07/12/2006, Regolamento recante identificazione dei dati sensibili e giudiziali trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del Dlgs 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali;
- Regolamento UE 2016/679, o GDPR
- D.lgs 196/2003 modificato dal D.lgs 101/18.

3. Strategie della scuola per garantire la sicurezza delle TIC

Al fine di garantire una gestione il più possibile corretta delle dotazioni tecnologiche in uso per la didattica, l'Istituto attua le seguenti strategie:

- II sistema informatico delle TIC della scuola viene regolarmente controllato in base alle norme di sicurezza;
- E' predisposta una separazione fisica tra la rete didattica e quella amministrativa;
- II sistema informatico della scuola è provvisto di un software antivirus aggiornato periodicamente;
- La connessione WiFi ad Internet dalle scuole è regolata da un meccanismo di autenticazione-autorizzazione;
- L'uso dei computer presenti e l'utilizzo dei laboratori informatici mobili è regolamentato come descritto nel presente documento.

Sono attivate strategie di informazione sull'uso consapevole della rete:

> avvio di percorsi di formazione ad un uso consapevole delle TIC rivolti agli insegnanti nel corso dell'anno scolastico;

> coinvolgimento dei genitori come partner educativi nei percorsi di formazione che riguardano gli studenti;

- > costante e aggiornata informazione agli utenti sui pericoli della rete in relazione all'evoluzione delle tecnologie in collegamento con le Forze di polizia e gli Enti preposti;
- > controllo (una tantum e/o all'evenienza di episodi dubbi) del sistema informatico (cronologia, temp, cookies, ecc.) da parte dei responsabili dell'attività informatica;
- > installazione di *firewall* sull'accesso Internet;
- > settaggio delle macchine in modo che agli utenti non sia consentito di scaricare ed installare da Internet alcun tipo di software ed utilizzare memorie di massa esterne quali drive memory, dischi removibili.

4. Descrizione delle infrastrutture tecnologiche

Pertanto, al fine del corretto utilizzo delle ICT nonché nell'ottica di una gestione efficiente ed efficace di tutto l'Istituto si rende necessario individuare tutte le risorse tecnologiche informatiche di cui l'Istituto dispone e regolamentarne il loro utilizzo.
L'Istituto Comprensivo Statale di Prevalle dispone di tecnologie informatiche sia per lo svolgimento delle attività didattiche e laboratoriali che per il funzionamento amministrativo.
L'Istituto dispone di due reti logicamente separate, utili per l'accesso a internet ed intranet, rispettivamente per l'aspetto amministrativo e didattico.

5. Postazioni informatiche e rete di Istituto: generalità

L'accesso alla rete dell'Istituto wireless da parte del personale docente e ATA è protetta da misure di sicurezza legate alla presenza di un titolo di accesso personale con doppio account (personale dipendente e personale esterno). Gli alunni delle scuole secondarie possono accedere alla rete wireless attraverso un accesso personale correlato univocamente ad una specifica apparecchiatura per un determinato periodo di tempo. Pertanto per accedervi deve essere utilizzata la propria specifica apparecchiatura, sotto la propria responsabilità.
E' fatto divieto di utilizzare la rete dell'Istituto per finalità non previste dal presente regolamento o non espressamente autorizzate. La navigazione è consentita nel rispetto delle seguenti condizioni:

a) è vietato connettere in rete stazioni di lavoro se non dietro esplicita e formale autorizzazione del responsabile del Settore indicato dal DS;
b) è vietato modificare le impostazioni di sistema delle stazioni di lavoro;
c) è vietato monitorare ciò che transita in rete se non nelle forme e nei limiti previsti nel presente regolamento e nel rispetto dei limiti previsti dalla Legge 300/70, Statuto dei lavoratori.
d) Per problemi correlati alla sicurezza della rete locale, l'Istituto dispone di un sistema di controllo, il firewall, che registra tutte le attività sulla rete; il fine è quello di individuare, in caso di necessità, eventuali utilizzi fraudolenti della rete di Istituto, della quale è direttamente responsabile il Dirigente Scolastico; infatti, come definito anche dalle linee guida del Garante, il datore di lavoro (il DS), secondo i poteri a lui affidati dalle norme del codice civile, articoli 2086, 2087 e 2104, può riservarsi di controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro; tuttavia, ciò deve essere fatto nel rispetto delle norme poste a tutela del lavoratore (ci si riferisce, in particolare, al divieto di installare "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" di cui all'art. 4 della legge 300 del 1970). Pertanto il datore di lavoro potrebbe, ad esempio, verificare se vi è stato indebito utilizzo della connessione ad Internet da parte del dipendente attraverso il controllo degli accessi e dei tempi di connessione, senza però indagare sul contenuto dei siti visitati.

5.1 Accesso alle postazioni informatiche

Tutti i docenti hanno il diritto di poter accedere alle tecnologie informatiche singolarmente, per la preparazione delle lezioni e per le attività connesse all'attività di insegnamento, e con gli studenti per le attività didattiche. I docenti che non hanno dei laboratori di riferimento possono richiedere, previa prenotazione, l'uso dei laboratori mobili o di singoli dispositivi elettronici. Il Dirigente scolastico all'inizio di ogni anno scolastico

nomina una referente (es. Responsabile tecnologie di plesso) responsabile delle prenotazioni dei laboratori e delle apparecchiature informatiche.
Su ciascun laboratorio sarà affisso il foglio settimanale delle ore impegnate. Il docente che avendo prenotato un laboratorio decida di non utilizzarlo, deve darne tempestiva comunicazione al docente di riferimento e/o al referente di plesso.

5.2 Utilizzo delle postazioni da parte dei docenti

I docenti che utilizzano laboratori e le postazioni informatiche hanno l'obbligo di vigilare sul corretto utilizzo delle stesse da parte degli studenti sia quando operano singolarmente che in gruppo. In particolar modo ogni docente è tenuto:

a) ad illustrare ai propri allievi le regole di utilizzo contenute nel presente documento;
b) a controllare che l'accesso degli alunni alla rete di Istituto avvenga sempre e solamente sotto la propria supervisione e unicamente con gli strumenti messi a disposizione dalla scuola;
e) a dare chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforma studenti ecc), condividendo con gli alunni la netiquette e vigilando sul rispetto della stessa;
d) ad assumersi la responsabilità della tracciabilità dell'utilizzo e del mantenimento in buono stato della strumentazione tecnologica da lui stesso e dagli alunni utilizzata, segnalando prontamente eventuali malfunzionamenti o danneggiamenti al referente informatico di plesso e/o all'assistente amministrativa addetta – ufficio acquisti;
e) a non divulgare le credenziali di accesso agli account (username e password) e/o, nel caso ne sia a conoscenza, alla rete wifi;
f) nel caso si sia effettuato l'accesso al proprio account dalla postazione di classe, non allontanarsi dalla eventuale postazione di lavoro, lasciandola incustodita, se non prima di aver effettuato la disconnessione;
g) non salvare sulla memoria locale della postazione di classe file contenenti dati personali e/o sensibili;
h) proporre agli alunni attività di ricerca di informazioni in rete fornendo opportunamente loro indirizzi dei siti e/o parole chiave per la ricerca cui fare riferimento (creati per la didattica, istituzionali e/o preventivamente verificati dall'insegnante stesso).

5.3 Utilizzo delle postazioni informatiche da parte degli studenti

Gli studenti possono utilizzare tutte le apparecchiature informatiche di cui l'Istituto comprensivo dispone, sotto la guida e vigilanza dei docenti referenti ed in conformità con il progetto educativo, nel rispetto del seguente regolamento.
Per gli studenti delle scuole secondarie di Prevalle e Villanuova, è disponibile l'accesso alla piattaforma Google Suite for Education, attraverso l'attivazione di un account personale con password. Dalla piattaforma è possibile scaricare e caricare compiti, materiali didattici, lezioni e comunicare con i docenti della propria classe.
Gli studenti possono interagire anche con il sito ufficiale della scuola dal quale è possibile visualizzare varie sezioni tra cui l'Albo d'Istituto e le comunicazioni relative all'anno scolastico in corso, cui può accedere qualunque utente della rete compresi i genitori.

Gli alunni imparano a:

- conoscere l'origine delle informazioni a cui si accede o che si ricevono;
- utilizzare fonti alternative di informazione per proposte comparate;
- ricercare il nome dell'autore, la data dell'ultimo aggiornamento del materiale e possibili altri link;
- rispettare i diritti d'autore e i diritti di proprietà intellettuale;
- usare i motori di ricerca;
- essere coscienti dei rischi a cui si espongono quando sono in rete. Devono essere educati a riconoscere e ad evitare gli aspetti negativi di Internet (siti che inneggiano alla violenza, il

razzismo e lo sfruttamento dei minori);

- residui di cibi e bevande possono danneggiare i computer e gli altri dispositivi (mouse, casse, etc): è quindi preferibile non bere e mangiare in laboratorio o mentre si utilizzano gli strumenti.

5.4 L'utilizzo da parte degli studenti delle apparecchiature elettroniche ed informatiche sia nei lavori di gruppo che negli interventi individuali avviene nel rispetto delle seguenti regole:

a) utilizzare le apparecchiature informatiche nonché l'accesso in rete, sempre sotto la supervisione del docente. Costituiscono eccezione i casi di comprovata necessità (situazioni di disabilità, certificazione dsa, particolari progetti) per i quali è possibile l'utilizzo a scuola del PC personale dell'alunno, previa autorizzazione del Dirigente Scolastico;
b) accedere all'ambiente di lavoro con il corretto account, non divulgandone le credenziali di accesso (username, password), e archiviare i propri documenti in maniera ordinata seguendo le indicazioni date dal docente;
e) in caso di riscontro di malfunzionamenti della strumentazione e/o di contatto accidentale con informazioni, immagini e/o applicazioni inappropriate comunicarlo immediatamente all'insegnante;
d) non eseguire tentativi di modifica della configurazione di sistema delle macchine;
e) accedere alla rete solo in presenza o con l'autorizzazione dell'insegnante responsabile dell'attività;
f) non utilizzare la strumentazione della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);
g) chiudere correttamente la propria sessione di lavoro.

5.5 In particolare modo gli studenti, al fine di favorire l'integrazione e l'accesso alle tecnologie informatiche anche ai compagni meno preparati, sono tenuti al rispetto delle seguenti buone passi (lotta al cyberbullismo):

a) rispettare le persone diverse per nazionalità, cultura, religione, sesso: il razzismo e ogni tipo di discriminazione sociale non sono ammessi;
b) non essere intolleranti con chi ha scarsa dimestichezza con le tecnologie informatiche o commette errori concettuali;
e) non rivelare dettagli o informazioni personali o di altre persone (indirizzi, numeri di telefono);
d) richiedere sempre il permesso ai genitori , in caso di minori, prima di iscriversi a qualche mailing-list o sito web che lo richieda;
e) non dare indirizzo e numero di telefono a persone incontrate sul web, in caso di minori, senza chiedere il permesso ai genitori (questo perché non si può avere la certezza dell'identità della persona con la quale si sta comunicando);
f) non prendere appuntamenti con le persone conosciute tramite web, in caso di minori, senza aver interpellato prima i genitori;
g) non inviare foto, filmati, o altro materiale riconducibile alla propria persona senza aver chiesto, in caso di minori, preventivamente il consenso dei propri genitori;
h) non inviare foto, filmati, o altro materiale riconducibile ad altre persone senza avere prima richiesto il consenso del diretto interessato, ovvero nel caso di minori il consenso dei rispettivi genitori;
i) riferire sempre a insegnanti e genitori se si è raggiunti in internet da immagini o scritti che infastidiscono;
j) se qualche studente dovesse venire a conoscenza che altri compagni non rispettano le suddette regole è opportuno parlane con gli insegnanti e con i genitori;
k) chiedere il permesso ai genitori, nell'ipotesi di minori che utilizzino postazioni internet nelle proprie abitazioni, ovvero agli insegnanti, nell'ipotesi di apparecchiature scolastiche, prima di

scaricare dal web materiale di vario tipo.

5.6 Utilizzo delle postazione da parte del personale Docente e ATA

II personale deve aver cura della propria postazione pc o delle eventuali postazioni alle quali ha accesso, rispettare il presente regolamento facendo particolare attenzione alle seguenti disposizioni:

a) utilizzare la postazione e il collegamento a internet solo per finalità di servizio;
b) evitare di lasciare le email o file personali sui computer o sul server della scuola;
c) ricordare di chiudere la connessione (e di spegnere il computer) alla fine della sessione di lavoro su Internet e disabilitare la navigazione su Internet del laboratorio (qualora sia stata attivata);
d) comunicare tempestivamente al responsabile indicato dal DS malfunzionamenti e anomalie;
e) non collegare alla rete e ai PC dispositivi propri e diversi da quelli in dotazione dell'Istituzione scolastica;
f) non modificare le impostazioni di sistema dei dispositivi in dotazione;
g) è compito del personale A.T.A. custodire le chiavi, aprire e chiudere i laboratori, mantenere adeguata pulizia dei locali.

5.7 Password e account d'ingresso alla rete

Le password di accesso alla rete nonché ai vari programmi in rete, sono attribuite dal Dirigente Scolastico. La connessione alla rete è fatta direttamente e segretamente dal responsabile della rete. Nell'ipotesi di comunicazione delle password all'utente lo stesso è tenuto a:

- conservare nella massima segretezza la parola di accesso alla rete ed ai sistemi e qualsiasi altra informazione legata al processo di autenticazione;
- scollegarsi dal sistema ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima;
- non lasciare un elaboratore incustodito connesso alla rete, può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso;
- chiedere la sostituzione della password nel caso si sospetti che la stessa abbia perso la segretezza;
- sostituire la password quando il sistema lo richiede, applicando le caratteristiche di complessità che verranno comunicate al momento di consegna della prima credenziale.

6. Dispositivi collegabili alla rete

Alla rete di istituto possono essere collegati solo dispositivi elettronici ed informatici di proprietà dell'Istituto. Su richiesta degli interessati, previa autorizzazione del Dirigente Scolastico, acquisito i parere del Responsabile protezione dati e dell'amministratore di sistema) per attività connesse all'attività didattica , possono essere connessi alla rete dispositivi anche di natura privata. In tale ipotesi, il personale che vorrà avvalersi di propri dispositivi collegabili alla rete dovrà comunicare la tipologia e le caratteristiche dei dispositivi al referente/responsabile della rete di Istituto. In ogni caso è ammesso l'utilizzo di massimo 1 dispositivo privato (portatili, tablet, Ipad).

7. Posta elettronica

La casella di posta elettronica gestita da postazioni presenti nell'Istituto, è uno strumento legato alla finalità dell'insegnamento e alle attività ad esso connesse. Il personale della scuola titolare di casella di posta elettronica è responsabile del corretto utilizzo della stessa (art.615 comma 5 e segg. c.p.). L'utilizzo della casella deve avvenire nel rispetto delle seguenti buone prassi

a) non aprire messaggi insoliti o provenienti da sconosciuti, per non correre il rischio di essere infettati da virus occorrerà cancellare i messaggi senza aprirli. Anche i messaggi provenienti da conosciuti possono contenere file eseguibili (quindi virus), pertanto bisogna fare attenzione alle estensioni, es. exe., escr, pif.,bat, cmd., questi ultimi non devono essere aperti se non conosciuta la provenienza;

b) bloccare messaggi che diffondono "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata), possono limitare l'efficienza del sistema postale;
e) utilizzare formato compresso nell'ipotesi di invio di file pesanti, a titolo di esempio *.zip *.rar *.jpg;
d) per l'invio di file ad altre istituzioni pubbliche o private è preferibile utilizzare un formato protetto da scrittura (ad esempio il formato Acrobat *.pdf);
e) prima di iscriversi a "mailing list" esterne bisogna verificare in anticipo se il sito sia affidabile;
f) cancellare dalla casella i documenti ritenuti inutili al fine di evitare l'occupazione di spazio di memoria.

8. Antivirus

II personale che accede alle postazioni informatiche della scuola deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico della scuola mediante virus o mediante ogni altro software aggressivo (ad esempio non aprire mail o relativi allegati sospetti, non navigare su siti non professionali ecc). A tal fine il personale è tenuto:

a) a controllare la presenza e il regolare funzionamento del software antivirus della scuola. Nel caso che il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer e segnalare l'accaduto al responsabile;
b) ogni dispositivo magnetico di provenienza esterna alla scuola dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, non dovrà essere utilizzato.

9. Sito web dell'Istituto

La responsabilità e la gestione del sito web dell'Istituto è del rappresentante legale, ovvero del Dirigente Scolastico. La gestione del sito può essere affidata dal Dirigente Scolastico ad un docente o al personale amministrativo dell'Istituto.
Il sito web (www.icprevalle.gov.it) si pone come strumento informativo interno ed esterno, di comunicazione di contenuti educativi e di attività didattico-formative. L'istituto detiene i diritti d'autore dei documenti prodotti in proprio o dei quali è stato chiesto e ottenuto il permesso di pubblicazione.
Nella pubblicazione di immagini degli alunni minorenni è necessaria la preventiva liberatoria da parte dei genitori. Anche in presenza di liberatoria, l'Istituto procede con la massima attenzione, preferendo pubblicare immagini a campo lungo, senza primi piani; immagini di gruppo in attività piuttosto che di singoli.
Il sito rispetta i requisiti di accessibilità per i disabili di cui alla L.9/1/2004.
Nel sito dell'Istituto sono presenti tutte le informazioni relative all'organizzazione della scuola pertanto il personale, studenti e genitori sono obbligati a consultare il sito in aggiunta e/o sostituzione delle comunicazioni fornite nelle forme tradizionali.
Tali informazioni sono raggruppate per aree di interesse:

- scuola
- segreteria
- didattica

nelle quali è possibile trovare la Carta dei Servizi, il P.T.O.F., il Regolamento di istituto, la Normativa Scolastica, la Modulistica…..
Dal sito è possibile anche collegarsi al registro elettronico, alla piattaforma amministrativa e ad altri siti utili del MIUR.

10. Registro elettronico

I docenti che interagiscono con il registro elettronico (piattaforma Spaggiari) oltre a quanto previsto nel presente documento, in materia di fruizione di tecnologie informatiche, devono rispettare le seguenti prescrizioni:

a) aggiornare tempestivamente il registro elettronico in tempo reale relativamente alle presenze degli alunni in classe, alle annotazione dei ritardi e delle assenze;
b) aggiornare tempestivamente, le valutazioni, gli argomenti delle lezioni ed altre eventuali annotazioni;
e) cambiare periodicamente le password, almeno ogni 3 mesi, rispettando la dimensione e la tipologia dei caratteri suggeriti dai docenti amministratori;
d) non lasciare incustodito il notebook, a maggior ragione se è attivo il collegamento alla piattaforma;
e) non comunicare le password ad altri ed evitare che le stesse siano presenti su supporti cartacei o digitali.

Le password devono essere predisposte nel rispetto delle seguenti tecniche:

- utilizzare il numero dei caratteri previsti dall'amministratore;
- evitare di utilizzare caratteri e dati facilmente riconducibili al titolare della password (es. nome/cognome, data di nascita, nome dei figli, hobby, nome ci persone care, ecc);
- memorizzare la password evitando supporti cartacei o digitali come promemoria.

I docenti collaboratori del dirigente e i coordinatori di classe hanno accesso a tutte le sezioni del registro elettronico.

11. Disposizioni sull'uso delle lavagne interattive multimediali (LIM) o videoproiettori interattivi e non.

L'uso di LIM e videoproiettori da parte degli alunni è consentito esclusivamente per scopi didattici, in presenza e sotto la guida di un docente, responsabile del comportamento degli allievi. Il docente che utilizza tali strumenti deve aver cura di rispettarne le procedure corrette.
Docenti ed alunni sono tenuti a non modificare in alcun modo le impostazioni predefinite della LIM/videoproiettori e del computer ad essa/o collegato.
La manutenzione e l'assistenza tecnica sono affidate esclusivamente ai referenti tecnici.
L'uso dei canali di youtube o simili è consentito solo ai docenti ed esclusivamente per fini didattici.
Al termine dell'attività scolastica (ultima ora) il proiettore deve essere spento, per evitare il consumo della lampada, per limitare al massimo possibile la spesa per la sua sostituzione.
Durante le lezioni utilizzare la funzione AV mute per i proiettori che la prevedano.
Qualora si riscontri un problema di funzionamento in una propria classe o in una classe diversa dalla propria, il docente è tenuto a darne pronta segnalazione direttamente o via mail al Referente tecnico e/o all'assistente amministrativa addetta agli acquisti.

12. Disposizioni per l'uso dei dispositivi personali degli alunni in classe

I dispositivi personali sono strumenti didattici che possono essere utilizzati a scuola per attività predisposte dagli insegnanti ed a casa per continuare tali attività, per svolgere compiti e/o studiare previa autorizzazione da parte del docente concordata preventivamente con la Dirigente Scolastica.
Ciò comporta l'assunzione di precise responsabilità per l' utilizzo e la conservazione.
Ogni alunno è tenuto al rispetto delle seguenti regole di gestione dei device a scuola:

- Prendersi cura del proprio device e non lasciarlo mai incustodito;
- Prima di lasciare la propria aula (per recarsi in palestra o in altri ambienti) o durante l'intervallo, riporre il proprio device nello zaino o nell'armadio di classe. L'insegnante o il collaboratore scolastico dovranno chiudere a chiave l'aula o l'armadio;
- Non dimenticarlo a casa, essendo materiale scolastico necessario;
- Caricarlo quotidianamente affinchè sia funzionante e prima di venire a scuola, poiché in classe non è

consentito caricare i device;

- Farne un uso esclusivamente didattico, evitando di sovraccaricarlo con programmi/app che non siano necessarie alla didattica o con contenuti non appropriati.
- Ascoltare le direttive degli insegnanti e svolgere le consegne date, senza prendere iniziative personali.
- Non utilizzare il device per attività non indicate o scopi non funzionali alla didattica;
- E' vietato modificare la configurazione dei device;
- Avvisare tempestivamente l'insegnante in caso di cadute e/o rotture del device.

Si precisa che un uso dello strumento inappropriato o non idoneo alla didattica e alle indicazioni degli insegnanti sarà sanzionato.

Si ricorda che l'inosservanza delle regole sopra esposte potrà pregiudicare l'efficienza delle attrezzature e l'utilizzo delle medesime.

13. Tutela della privacy: garanzie generali

I trattamenti di dati personali effettuati dall'Istituto vengono posti in essere nel rispetto delle norme in materia di sicurezza e riservatezza: Regolamento UE 2016/679, D.Lgs. 196/03 (modificato da D.Lgs.101/18), Circolare AGID 1/2017, provvedimenti del Garante per la protezione dei dati personali.

Titolare dei trattamenti è il Dirigente Scolastico, il quale si è avvalso della facoltà di nominare responsabile dei trattamenti del personale e di segreteria il D.S.G.A.

Sono state autorizzate al trattamento dei dati le unità organizzative: segreteria, docenti, collaboratori scolastici, collaboratori del dirigente, organi collegiali. Inoltre sono stati autorizzate le diverse funzioni strumentali e, in genere, il personale che riveste un ruolo specifico per il quale sia necessaria un autorizzazione al trattamento di categorie particolari di dati personali.

Sono stati assegnati i ruoli di responsabile protezione dati e di amministratore di sistema.

Le misure di sicurezza adottate sono conformi alle indicazioni AGID 2017 e sono state valutate e modificate tenendo conto della complessità della struttura e delle innovazioni tecnologiche intervenute e adottate.

Son state adottate le informative per i trattamenti istituzionali ai sensi dell'articolo 13 del GDPR per i seguenti trattamenti; personale e collaboratori, alunni e famiglie, fornitori. In caso vengano posti in essere trattamenti per esigenze organizzative con modalità che prevedono la raccolta del consenso da parte degli interessati, vengono predisposti moduli idonei per ogni necessità.

13.1 Tutela della privacy: norme concernenti il personale della scuola

Le regole alle quali il personale dell'Istituto deve attenersi sono quelle contenute nel modulo R2 allegato alla determina autorizzativa dell'unità organizzativa di appartenenza, che di seguito riportiamo:

R2.1 istruzioni generali

Gli Incaricati devono attenersi rigorosamente a tutte le regole dettate dalla normativa di riferimento (ad oggi D.Lgs.196/2003 o Codice, Regolamento UE 2016/679 o GDPR, provvedimenti del Garante, codice AgID) e in particolare ai seguenti punti fondamentali:

L'obbligo di mantenere il dovuto **riserbo in ordine alle informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico**, deve permanere **in ogni caso**, anche quando sia venuto meno l'incarico stesso (art.326 del codice penale e art. 28 della legge 241/90).

Ai sensi dell'art. 29 del GDPR e dell'articolo 2-quaterdieces del Codice gli Incaricati del trattamento devono operare sotto la diretta autorità del Titolare (o del Responsabile, se nominato) e devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni impartite.

Finalità del trattamento: il trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo

svolgimento delle funzioni istituzionali.

Modalità di trattamento dei dati: Può essere effettuato **manualmente,** mediante **strumenti informatici, telematici o altri supporti.** Ai sensi del GDPR, il trattamento deve applicare il principio **di pertinenza e non eccedenza** rispetto alle finalità del trattamento medesimo, pertanto è consentita l'acquisizione dei soli dati personali strettamente indispensabili per adempiere alle finalità richieste dall'interessato. Ogni acquisizione di dati dev'essere preceduta dall'apposita informativa all'Interessato di cui all'art. 13 del GDPR, avendo cura nel caso di documenti ritenuti potenzialmente classificabili come sensibili o giudiziari di fare espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento.

I dati devono essere trattati in modo **lecito e secondo correttezza,** devono essere **esatti ed aggiornati.**

È vietata all'Incaricato qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia funzionale allo svolgimento dei compiti affidati.

Per il trattamento devono essere seguite le norme di legge in materia di tutela della riservatezza dei dati personali e devono essere applicate le misure di protezione previste dal Titolare.

Categorie di soggetti ai quali i dati possono essere comunicati: la comunicazione da parte della scuola ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. La comunicazione da parte della scuola a privati o a enti pubblici economici e la diffusione sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Modalità di trattamento dei dati sensibili/giudiziari: Ferma restando l'applicazione delle disposizioni vigenti in materia di trattamento dei dati sensibili e giudiziari e delle istruzioni impartite dal Titolare e dal Responsabile del trattamento, i documenti (anche tuttora in lavorazione e non definitivi) ed i supporti recanti dati sensibili o giudiziari devono essere conservati in elementi di arredo o ambienti muniti di serratura e non devono essere lasciati incustoditi in assenza dell'incaricato.

Trattamenti di dati inerenti la salute: i supporti ed i documenti recanti dati relativi alla salute, dati genetici o biometrici e dati relativi alle abitudini sessuali devono essere conservati separatamente dai dati comuni, preferibilmente in contenitori muniti di serratura.

R2.2 regole di comportamento

E' fatto divieto di:

- portare al di fuori della sede di lavoro documenti, copie di documenti, tabulati, registrazioni audio o video che contengano dati riferibili ad un soggetto identificabile, tranne per le operazioni autorizzate che lo richiedano espressamente;
- fare parola con altri al di fuori dei soggetti come Lei incaricati al trattamento o di soggetti aventi diritto di conoscenza dei dati in questione;
- utilizzare gli strumenti, anche informatici, che Le sono messi a disposizione per organizzare elenchi, inviare corrispondenza, ricavare statistiche, al di fuori di quelle che siano strettamente necessarie per lo svolgimento dei compiti che Le vengono assegnati;
- utilizzare in qualsiasi modo a vantaggio Suo o di terzi le informazioni con le quali viene a contatto nello svolgimento delle Sue mansioni;
- fornire informazioni, anche verbali, a terzi non incaricati senza essersi preventivamente accertato del diritto del richiedente alla conoscenza ovvero del consenso da parte dell'interessato a che la comunicazione avvenga;
- affidare ad altri soggetti non nominati a loro volta incaricati del trattamento elaborazioni sui dati di Sua competenza.
- assicurarsi che quando parla con altri, personalmente o per telefono, relativamente a dati o situazioni tramite le quali sia identificabile un soggetto tutelato non siano presenti nell'ambiente terzi che non siano a loro volta incaricati del trattamento;
- nel caso di invio tramite fax di documenti o tabulati assicurarsi che la copia venga ricevuta immediatamente dal destinatario, specialmente se vengono inviati dati "sensibili" (documenti dai quali risultino informazioni relative alla salute, alle convinzioni religiose, filosofiche, politiche, abitudini sessuali, razza, etnia, dati riferiti al casellario giudiziario). Se non si riesce ad avere questa certezza astenersi dall'invio e cercare soluzioni alternative. In ogni caso applicare sempre la procedura relativa alle comunicazioni che le verrà consegnata.
- i documenti vanno utilizzati prevalentemente negli ambienti deputati alle elaborazioni. Quando si renda necessario l'utilizzo in altri ambienti non lasciare i documenti incustoditi e, al termine, riportarli nel luogo dove devono essere conservati;
- nei luoghi di lavoro ai quali possono accedere anche soggetti non incaricati non lasciare i documenti accessibili in caso di assenza ma riporli nei dispositivi deputati (armadi, cassetti, classificatori). Ove sia prevista la chiusura con chiave dei dispositivi di conservazione fare in modo che venga utilizzata e che venga poi riposta nei modi che il responsabile indicherà;
- nei luoghi di lavoro non accessibili al pubblico non assentarsi senza avere chiuso i locali. Nel caso si fosse impossibilitati a chiudere, assicurarsi che i documenti siano stati riposti;
- in caso il trattamento preveda lo spostamento dei documenti ad altra sede, fare in modo che il trasporto avvenga in regime di sicurezza: non lasciare i documenti incustoditi (in macchina, sui mezzi pubblici), non lasciare i documenti visibili da altri, non affidare a terzi, se non autorizzati, il trasporto;
- in caso di richiesta verbale, telefonica o scritta di dati riferibili ad un interessato assicurarsi che il richiedente sia autorizzato, ovvero che sussista un obbligo di legge, che esista un contratto con l'interessato che preveda la comunicazione a quel soggetto, che l'interessato abbia già espresso il suo consenso. Se possibile documentare la legittimità della richiesta e tenere la copia agli atti nel registro delle attività (tenuto dal Responsabile);
- se la comunicazione descritta al punto precedente non fosse consentita valutare con il Responsabile se sia il caso di richiedere una apposito consenso all'interessato. In tal caso raccogliere il consenso in forma scritta e consegnarlo al Responsabile che provvederà a conservarlo nel registro delle attività;

- i documenti, o copie di essi, che non vengono più utilizzati devono essere distrutti ovvero resi illeggibili prima del loro cestinamento;
- per ogni situazione di potenziale rischio che non sia stata prevista fare riferimento al Responsabile competente e chiedere l'integrazione delle istruzioni.

La mancata osservanza di tali disposizioni darà luogo alle sanzioni previste per legge.

13.2 Privacy e famiglie

Le famiglie possono consultare solo voti e informazioni riguardanti il soggetto interessato.
Ogni studente o genitore per entrare nel sistema deve obbligatoriamente inserire i suoi personali username e password.
Non possono essere presenti due utenti con la stessa username.
E' assolutamente vietato cedere password, ovvero consentire ad altri soggetti di effettuare operazioni in nome e per conto del titolare di una password.
Nell'ipotesi di conoscenza accidentale di dati e/o informazioni riguardanti altri soggetti (alunni, famiglie, docenti e altro personale o non della scuola) è assolutamente vietata la divulgazione, pubblicazione o qualsiasi altra operazione. La mancata osservanza di tali disposizioni darà luogo alle sanzioni previste per legge.

14. Diritto d'autore

II Diritto di autore è regolato dalla legislazione vigente sui Diritti d'Autore: Legge del 22 aprile 1941 n° 633 art. 70 di cui si riporta un estratto: "*... il riassunto, la citazione o la riproduzione di brani o diparti di opera per scopi di critica di discussione ed anche di insegnamento, sono liberi nei limiti giustificati da tali finalità e purché non costituiscano concorrenza all'utilizzazione economica dell'opera".* Se nel realizzare lavori didattici o pagine web, l'autore inserisce a scopo di discussione, di critica, di informazione culturale, parti di opere, brevi estratti o citazioni menzionando il nome dell'autore e la fonte, non incorre in problemi di copyright.

In base alle vigenti norme sul diritto d'autore è vietato utilizzare le risorse dell'Istituto per:
- copiare/fotocopiare qualunque tipo di materiale, protetto da copyright;
- scaricare o duplicare CD e DVD, protetti da copyright.

15. Disposizioni di legge e sanzioni

Al di là delle regole di buona educazione ci sono comportamenti, talvolta solo apparentemente innocui, che possono portare gli autori a commettere veri e propri reati e, di conseguenza, a subire procedimenti penali dalle conseguenze molto serie. Alcuni esempi:

Reati informatici

LA LEGGE 547/93 individua e vieta tutta una serie di comportamenti nell'ambito informatico e che sono stati reputati lesivi per gli interessi non solo di singoli privati cittadini ma anche di persone giuridiche, in particolare per le imprese e gli enti pubblici:
- Danneggiamento informatico
- Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
- Frode informatica

Reati non informatici

Sono da considerare reati non informatici tutti quei reati o violazioni del codice civile o penale in cui il ricorso alla tecnologia informatica non sia stato un fattore determinante per il compimento dell'atto:
- Ingiuria
- Diffamazione
- Minacce e molestie.

Atti di vandalismo, di sabotaggio o furti, verranno perseguiti nelle forme previste, compreso il risarcimento degli eventuali danni arrecati.

A fronte di violazioni delle regole stabilite dalla politica scolastica, la scuola, su valutazione del responsabile di laboratorio e del Dirigente Scolastico, si assume il diritto di impedire l'accesso dell'utente a Internet per un certo periodo di tempo, rapportato alla gravità.
La violazione o il dolo accertati, oltre all'intervento disciplinare del consiglio di classe, daranno luogo alla richiesta di risarcimento delle ore perse per ripristinare il sistema e renderlo nuovamente operante ed affidabile; rimangono comunque applicabili ulteriori sanzioni disciplinari, azioni civili per danni, nonché l'eventuale denuncia del reato all'autorità giudiziaria.
Nel caso di infrazione consapevole da parte dei docenti o del personale non docente si interverrà per via amministrativa secondo le norme vigenti.

16. Norme conclusive

"Le linee guida per l'uso delle risorse tecnologiche e di rete" sono allegate al Regolamento di Istituto e pubblicato all'albo on line della scuola.
Il Dirigente scolastico ha il diritto di revocare l'accessibilità temporanea o permanente ai laboratori informatici e/o all'utilizzo di strumenti tecnologici (tablet, notebook, ecc) a chi non si attiene alle regole stabilite.
I genitori/tutori ed il personale scolastico vengono informati della pubblicazione del presente documento

L'Indirizzo mail per eventuali segnalazioni è: BSIC86700Q@ISTRUZIONE.IT

ALLEGATO: NETIQUETTE

Materiale utile scaricabile, del Garante per la privacy disponibile sul sito http://www.garanteprivacv.it/socialprivacy

ALLEGATO A: NETIQUETTE

Fra gli utenti dei servizi telematici di rete si è sviluppata, nel corso del tempo, una serie di tradizioni e di norme di buon senso che costituiscono la "Netiquette" che si potrebbe tradurre in "Galateo (Etiquette) della Rete (Net)": il Galateo della rete.

l. Non essere offensivo - II testo è l'unico mezzo attraverso il quale comunicare con gli altri in rete. Il tono della voce, l'espressione del viso, non possono essere di aiuto per far comprendere all'altro il senso del discorso. Il rischio di essere fraintesi è altissimo. Bisogna tenerlo sempre presente quando si scrive e usare gli emoticons per ribadire il tono del messaggio: scherzoso, allegro o triste e così via.

2. Seguire regole di comportamento analoghe alle proprie regole di vita - Utilizzare in maniera fraudolenta un prodotto a pagamento equivale ad un furto. Solo acquistandolo regolarmente s'incoraggiano i realizzatori a creare altri prodotti.

3. Scegliere l'ambiente adatto a se stessi - Ogni chat, mailing list, newsgroup, forum ha delle caratteristiche specifiche e non si può trovare sempre argomenti adatti a noi o di nostro interesse. Scegliere la community che si avvicina di più alle proprie esigenze, ma soprattutto quella dove ci si sente più a nostro agio, anche grazie al controllo del moderatore.

4. Scegliere di essere paziente e comprensivo - Quando s'invia un messaggio non bisogna pretendere risposta. Chi comunica con noi può non essere interessato all'argomento che proponiamo oppure può non avere il tempo di rispondere.

5. Scegliere toni moderati - Se si esprime il parere in maniera pacata, è meno probabile che le parole usate possano provocare reazioni dure da chi comunica con noi. Basta poco per infiammare una discussione e serve invece molto tempo per tornare ad un dialogo tranquillo.

ó. Rispettare la privacy - Usare in rete la stessa regola che usi nella vita. Ognuno di noi ha il diritto di scegliere se condividere o meno le informazioni che lo riguardano.

7. Non abusare delle proprie conoscenze - Non usare mai le proprie competenze per entrare nel mondo altrui.

8. Trascurare gli errori degli altri - II desiderio di rispondere velocemente porta a errori di digitazione, di grammatica o di sintassi ma l'importante è che il messaggio sia compreso.

9. Dimenticare le differenze - La rete è un mondo nel quale l'unico strumento è la tastiera, l'unico oggetto visibile il monitor. Non ha nessuna importanza il colore della tua pelle, la tua religione.

10. Presentarsi con cura - In rete si hanno solo le parole per farsi conoscere. Bisogna usarle con cura, scegliendo quelle di cui si è veramente convinti, solo così daremo a chi comunica con noi l'impressione di come siamo veramente.

11. Utilizzare la rete per ampliare le tue conoscenze - Internet è una sterminata enciclopedia a portata di mouse ed offre anche la possibilità di leggere le opinioni degli altri su qualsiasi argomento. Si possono trovare informazioni specialistiche, il materiale per una ricerca scolastica ma anche solo confrontare la propria opinione.

12. Essere prudente - Non dare in modo affrettato informazioni personali o che riguardano propria famiglia. Non accettare senza riflettere di incontrare qualcuno che si é appena conosciuto nella rete. Non credere a tutto quello che viene detto.

13. Non urlare - Scrivere in maiuscolo su Internet equivale ad urlare: è uno strumento a disposizione per enfatizzare le cose che stai dicendo. Attenzione a non abusarne.

La Dirigente Scolastica
Prof.ssa Maria Vittoria Papa

"*Documento informatico firmato digitalmente ai sensi del D.Lgs 82/2005 CAD (art. 45 –Valore giuridico della trasmissione), ss.mm.ii e norme collegate"*