Istituto d'Istruzione Superiore Secondaria Statale
"*Eugenio Pantaleo*"
*già istituito con D.P.R. n° 1284 del 30/09/1953*
*Settore ECONOMICO Indirizzi: Amministrazione Finanza e marketing – Sistemi Informativi Aziendali – Relazioni Internazionali per il Marketing*
*Settore TECNOLOGICO Indirizzi: Informatica - Telecomunicazioni – Costruzioni Ambiente e Territorio - Chimica Materiali e Biotecnologie*
*Settore ALBERGHIERO: Servizi di Enogastronomia e Ospitalità Alberghiera*
Cod. Fisc.: 95215890633 ~ Via Cimaglia 96 - 80059 Torre del Greco ~ Tel./Fax 081-8812241
E-MAIL: NAIS12800T@istruzione.it; PEC: NAIS12800T@pec.istruzione.it; SITO: www.iissspantaleo.edu.it
*Preparati oggi ad affrontare il domani*

# INFORMATIVA "SICUREZZA INFORMATICA"

## LINEE GUIDA PER L'USO DELLE RISORSE TECNOLOGICHE E DI RETE

### Scopi di una politica di uso sicuro delle risorse tecnologiche

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.

Lo sviluppo delle competenze digitali è uno degli obiettivi base del quadro europeo delle competenze chiave per l'apprendimento permanente. Naturalmente, rappresenta una delle principali competenze da acquisire nell'ambito del curricolo di Istituto.

Inoltre, il curricolo scolastico prevede che gli alunni imparino a cercare informazioni e materiale didattico, creare e condividere documenti e scambiare informazioni attraverso l'utilizzo delle tecnologie e degli strumenti digitali applicati alla didattica. La rete Internet offre sia agli alunni che ai docenti 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 e degli Strumenti Digitali 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.

Il personale di segreteria, nella gestione degli aspetti amministrativi dell'Istituto fa largo uso delle tecnologie informatiche, nell'ottica della dematerializzazione degli atti oltre che per una efficiente ed efficace comunicazione.

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.

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 nellarete, 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;
- garantire il rispetto delle leggi in materia di protezione dei dati.

**Riferimenti normativi**

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

- L. 547/ 1993: norme in materia di reati informatici;
- 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;
- L. 325/2000 sull'adozione delle misure di sicurezza nel trattamento dei dati in applicazione dell'alt. 15 della L. 675/1996;
- 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. 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);
- L. 107/2015, che tra gli obiettivi educativi prioritari pone lo sviluppo delle competenze digitali e l'adozione del Piano Nazionale della Scuola Digitale;
- Regolamento UE 2016/679, Regolamento generale sulla protezione dei dati personali;
- L. 71/2017, Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo;
- Nota 482 del 18 febbraio 2021, Linee di Orientamento per la prevenzione e il contrasto del Bullismo e del Cyberbullismo;
- L. 92/2019, Introduzione all'insegnamento dell'educazione civica.

**Strategie della scuola per garantire la sicurezza informatica**

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

- il sistema informatico dell'Istituto viene regolarmente controllato in base alle norme di sicurezza;
- è predisposta una separazione logica tra la rete didattica e quella amministrativa;
- il sistema informatico della scuola è provvisto di un software antivirus aggiornato periodicamente;
- la connessione WiFi ad Internet dell'Istituto è regolata da un meccanismo di autenticazione-autorizzazione e da tecniche di filtraggio;

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

- avvio di percorsi di formazione ad un uso consapevole delle tecnologie digitali rivolti ai docenti;
- 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;
- utilizzo di firewall e proxy;
- settaggio delle macchine in modo che agli utenti non sia consentito di scaricare e/o installare alcun tipo di software.

**Descrizione delle Risorse**

Al fine del corretto utilizzo 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 regolamentare il loro utilizzo.

L'Istituto dispone di tecnologie informatiche sia per lo svolgimento delle attività didattiche e laboratoriali che per il funzionamento amministrativo:

- laboratori informatici provvisti di una postazione per ogni studente (con accesso cablato alla rete Intranet e Internet);
- aule attrezzate provviste di postazione per il docente (con accesso cablato alla rete Intranet e Internet) e sistema di videoproiezione e/o lavagna interattiva multimediale;
- kit di proiezione portatili, comprensivi di PC e videoproiettore (con accesso wireless alla rete Internet);
- laboratori mobili (con accesso wireless alla rete Internet);
- uffici con postazioni fisse per il personale amministrativo e tecnico (con accesso cablato alla rete Intranet e Internet);
- postazioni per il personale ausiliario (con accesso cablato alla rete Internet);
- stampanti di rete (disponibili previo accounting);
- notebook (con accesso wireless alla rete Internet) a disposizione di docenti e studenti per l'utilizzo legato ad attività temporanee e di breve durata.

L'Istituto dispone di due reti logicamente separate, utili per l'accesso a Internet, rispettivamente per l'aspetto amministrativo e didattico.

**1 - Postazioni informatiche e rete di Istituto: generalità**

L'accesso alle postazioni fisse e alla rete Intranet da parte del personale e degli studenti è vincolata da un sistema di accounting personale.

Anche l'accesso alla rete wireless da parte del personale docente e ATA è protetto da misure disicurezza legate ad un sistema di accounting personale.

Gli alunni non possono accedere alla rete wireless, se non limitatamente all'effettuazione di attività specifiche (dietro richiesta del docente di riferimento) e comunque legate ad un sistema di accounting personale.

È 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. utilizzo della rete per i soli scopi legati alle attività didattico -amministrative;

b. rispetto della netiquette (si veda l'allegato "Netiquette - etica e norme di buon uso dei servizi di rete");

c. divieto di monitoraggio di ciò che transita in rete se non nelle forme e nei limiti previsti nel presente regolamento.

Per problemi correlati alla sicurezza della rete locale, l'Istituto dispone di un sistema di controllo (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 riservarsidi controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumentidi 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.

**2 - Accesso alle postazioni informatiche**

Tutti i docenti hanno il diritto di poter accedere alle postazioni singolarmente, per le attività connesse alla funzione docente, 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 dei kit di proiezione o dei singoli notebook.

**2.1 - Utilizzo delle postazioni da parte dei docenti**

I docenti che utilizzano le postazioni informatiche (o nelle aule didattiche o i kit di videoproiezione) sono tenuti a:

a. assumersi la responsabilità della tracciabilità dell'utilizzo e del mantenimento in buono stato della strumentazione tecnologica da loro stessi utilizzata, segnalando prontamente eventualimalfunzionamenti agli assistenti tecnici (tramite l'utilizzo di modulo predisposto o tramite chiamata diretta);

b. segnalare prontamente eventuali danneggiamenti o mancanze all'ufficio tecnico;

c. non divulgare le credenziali di accesso (ai dispositivi fissi, alla rete wi-fi, alle caselle di posta istituzionali, al captive portal per l'accesso a Internet, al sistema di prenotazione aule, al registro elettronico, a piattaforme didattiche);

d. dopo aver effettuato l'accesso al proprio account, non allontanarsi dalla eventuale postazione di lavoro, lasciandola incustodita, senza aver effettuato la disconnessione;

e. non salvare sulla memoria locale dei dispositivi dell'Istituto file, soprattutto se contengono dati personali e/o sensibili;

f. collegare dispositivi di memorizzazione portatili personali solo previa scansione con software antivirus apposito;

g. utilizzare le strumentazioni (PC, stampanti, webcam) e l'accesso alla rete Intranet ed Internet dell'Istituto per le sole finalità connesse alla funzione docente;

h. utilizzare le sole caselle di posta elettronica istituzionali (@iissspantaleo.edu.it e @posta.istruzione.it);

i. conoscere le regole base di protezione dai rischi derivanti dall'utilizzo della rete (phishing, spam, ...);

j. scaricare materiale digitale per fini personali e/o protetto da copyright;

k. visitare siti non necessari ad una normale attività didattica.

I docenti che utilizzano i laboratori (anche mobili) 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 (si sottolinea che tutti gli studenti seguono unità formative specifiche sulla sicurezza dei laboratori);

b. a controllare che l'accesso degli alunni alla rete Internet avvenga sempre e nel rispetto del presente Regolamento;

c. a dare chiare indicazioni sul corretto utilizzo della rete (Internet, piattaforme online,...), 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 agli assistenti tecnici tramite chiamata diretta);

e. segnalare prontamente eventuali danneggiamenti o mancanze all'ufficio tecnico;

f. a sollecitare gli alunni a non divulgare le credenziali di accesso (ai dispositivi fissi, alla casella di posta istituzionale, al registro elettronico, a piattaforme didattiche);

g. dopo aver effettuato l'accesso al proprio account, non allontanarsi dalla eventuale postazione di lavoro, lasciandola incustodita, senza aver effettuato la disconnessione;

h. non salvare sulla memoria locale dei dispositivi dell'Istituto file contenenti dati personali e/o sensibili;

i. collegare dispositivi di memorizzazione portatili solo previa scansione con software apposito

j. utilizzare gli strumenti (PC, stampanti, webcam) e l'accesso alla rete Intranet ed Internet dell'Istituto per le sole finalità connesse alla funzione docente

k. utilizzare le sole caselle di posta elettronica istituzionali (@iissspantaleo.edu.it e @posta.istruzione.it)

l. conoscere le regole base di protezione dai rischi derivanti dall'utilizzo della rete (phishing, spam, ...)

m. proporre agli alunni attività di ricerca di informazioni in rete principalmente fornendo loro, almeno inizialmente quale opportuno riferimento guida, 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).

E' compito del personale Ausiliario custodire le chiavi, aprire e chiudere i laboratori.

Copia delle chiavi di ogni laboratorio viene custodito anche nell'ufficio degli assistenti tecnici.

**2.2 - Utilizzo delle postazioni informatiche da parte degli studenti**

Gli studenti possono utilizzare tutti i dispositivi elettronici (PC dei laboratori e della biblioteca,notebook portatili, notebook tablet dei laboratori mobili) di cui l'Istituto dispone, sotto la guida e vigilanza dei docenti referenti ed in conformità con il progetto educativo, nel rispetto del seguente regolamento e dell'allegato "Regolamento di gestione e utilizzo dei Laboratori Didattici e delle Strumentazioni Tecnologiche

Per gli studenti, è disponibile l'accesso alla piattaforma Google Workspace for Education, attraverso l'attivazione di un account personale con password. Dalla piattaforma è possibile scaricare e caricare compiti.

Gli studenti hanno accesso al Registro Elettronico, attraverso l'attivazione di un account personale con password. Attraverso il registro elettronico è possibile visualizzare comunicazioni, compiti, note, voti, assenze.

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.

**L'utilizzo da parte degli studenti dei dispositivi digitali sia nei lavori di gruppo che nelle attività individuali avviene nel rispetto delle seguenti regole:**

a. utilizzare i dispositivi nonché l'accesso in rete, sempre sotto la supervisione del docente;
b. accedere all'ambiente di lavoro con il proprio account personale;
c. assumersi la responsabilità della tracciabilità dell'utilizzo e del mantenimento in buono stato della strumentazione tecnologica da loro stessi utilizzata, segnalando prontamente eventuali malfunzionamenti, danneggiamenti o mancanze al docente di riferimento
d. non divulgare le credenziali di accesso (ai dispositivi fissi, alla casella di posta istituzionale, a Internet, al registro elettronico, a piattaforme didattiche);
e. dopo aver effettuato l'accesso al proprio account, non allontanarsi dalla eventuale postazione di lavoro, lasciandola incustodita, senza aver effettuato la disconnessione;
f. archiviare i propri documenti in maniera ordinata nella propria cartella di rete e non nella memoria locale del dispositivo;
g. non eseguire tentativi di modifica della configurazione di sistema delle macchine;
h. non eseguire tentativi di monitoraggio dei dati presenti nella rete:
i. accedere alla rete solo in presenza o con l'autorizzazione dell'insegnante responsabile dell'attività;

j. non utilizzare i dispositivi e l'accesso a Internet della scuola a scopi personali, ludici e/o ricreativi (a meno che l'attività didattica non lo preveda esplicitamente);

k. chiudere correttamente la propria sessione di lavoro;

l. collegare dispositivi di memorizzazione portatili solo previa scansione con software antivirus apposito;

m. utilizzare la sola casella di posta elettronica istituzionale (@iissspantaleo.edu.it);

n. conoscere le regole base di protezione dai rischi derivanti dall'utilizzo della rete (phishing, spam, ...)

o. scaricare materiale digitale per fini personali e/o protetto da copyright;

p. visitare siti non necessari ad una normale attività didattica

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 prassi (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;

c. 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 rispettivigenitori;

i. riferire sempre a insegnanti e genitori se si è raggiunti in rete da immagini o scritti che infastidiscono;

j. se qualche studente dovesse venire a conoscenza che altri compagni non rispettano le suddette regole è opportuno parlarne con gli insegnanti e con i genitori;

k. chiedere il permesso ai genitori, nell'ipotesi di minori che utilizzano postazioni internet nelle proprie abitazioni, ovvero agli insegnanti, nell'ipotesi di apparecchiature scolastiche, prima di scaricare dal web materiale di vario tipo;

l. seguire le regole della Netiquette (si veda l'allegato "Netiquette - Etica e Norme di buon uso dei servizi di rete").

**2.3 - 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. verificare mediante il software antivirus presente nei dispositivi ogni dispositivo di provenienza esterna alla scuola prima del suo utilizzo e, nel caso venga rilevato un virus non eliminabile dal software, il dispositivo non dovrà essere utilizzato.

b. 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 agli assistenti tecnici informatici;

**3 – Account di Istituto per l'utilizzo di Google Workspace**

L'account istituzionale (nome.cognome@iissspantaleo.edu.it il personale, e nome.cognome@iissspantaleo.edu.it per gli studenti), è uno strumento legato alla finalità didattico-amministrative e alle attività ad esso connesse. Il personale della scuola titolare di casella di account di Istituto è responsabile del corretto utilizzo della stessa (art.615-quater c.p.).

L'utilizzo dello stesso, in particolar modo della casella di posta elettronica, deve avvenire nel rispetto delle seguenti buone prassi

a. utilizzare l'account solo per scopi professionali;

b. non aprire messaggi di posta elettronica 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 dei file allegati (anche questi ultimi non devono essere aperti);

c. bloccare messaggi che diffondono "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata);

d. per l'invio di file ad altre istituzioni pubbliche o private è preferibile utilizzare un formato protetto da scrittura;

e. utilizzare l'account per l'iscrizione a mailing list o piattaforme solo per uso professionale

f. cancellare dall'account i documenti ritenuti inutili al fine di evitare l'occupazione di spazio di memoria.

**4 - 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 è affidata dal Dirigente Scolastico ad un docente, indicato come "referente del sito web di Istituto".

Il sito web (www.iissspantaleo.edu.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, in parte, i requisiti di accessibilità per i disabili di cui alla L.9/1/2004 (si veda dichiarazione di accessibilità reperibile al link… )

Nel sito dell'Istituto sono presenti tutte le informazioni relative all'organizzazione della scuola: P.T.O.F., Regolamenti d'istituto, contatti,…

**5 - Registro Elettronico**

I docenti che interagiscono con il registro elettronico (NUVOLA - Madisoft) 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 annotazioni dei ritardi e delle assenze;

b. aggiornare tempestivamente, le valutazioni, gli argomenti delle lezioni ed altre eventuali annotazioni;

c. cambiare periodicamente le password, rispettando la dimensione e la tipologia dei caratteri suggerite dalla piattaforma;

d. non lasciare incustoditi dispositivi in cui è attivo il collegamento alla piattaforma;

e. non comunicare la password di accesso ed evitare che le stesse siano presenti su supporti cartacei o digitali;

f. non memorizzare nel browser di dispositivi (personali e non) la password di accesso.

**6 - Struttura del Sistema Informatico**

**Rete Cablata**

Il sistema informativo dell'Istituto è composto da due reti (didattica e amministrativa) logicamente separate, che condividono solamente l'accesso esterno alla rete Internet.

L'account permette l'accesso ai PC fissi presente nell'Istituto (per docenti e studenti nell'area didattica, per il personale nell'area amministrativa).

**Rete Wireless**

Tutte le sedi dell'Istituto sono coperte da segnale Wireless.

**Tracciamento e Monitoraggio**

Per quanto riguarda la rete cablata, il tracciamento della navigazione avviene attraverso un sistema di firewall.

Il monitoraggio della rete wireless avviene in tempo reale attraverso il controller wi-fi di rete che quantifica dispositivi collegati in quel momento.

**Manutenzione**

Tutti i dispositivi dell'istituto vengono controllati costantemente sia in termini di funzionalità che di sicurezza.

I dispositivi mobili, i kit di videoproiezione vengono controllati periodicamente, ad intervalli regolari, dagli assistenti tecnici informatici

**7 - Accounting degli Utenti**

Personale, studenti e genitori sono proprietari di differenti account relativi al sistema informativo di Istituto.

**Docenti:**

- Google Workspace: account per l'accesso ai servizi della Google Workspace (@iissspantaleo.edu.it);
- Registro Elettronico: account per l'accesso al registro elettronico (NUVOLA - Madisoft);
- Account per l'accesso alla rete wireless;

**Personale Amministrativo:**

- Account che permette l'accesso ai dispositivi fissi appartenenti alla rete amministrativa;
- Google Workspace: account per l'accesso ai servizi della Google Workspace (@iissspantaleo.edu.it);
- Registro Elettronico: account per l'accesso al registro elettronico (NUVOLA - Madisoft)
- servizio di stampa: PIN per l'utilizzo dei fotocopiatori;
- portali ministeriali: alcuni assistenti amministrativi hanno accesso a portali ministeriali particolari, a seguito di funzioni facenti parte dell'incarico ricoperto.

**Personale Tecnico:**

- Account che permette l'accesso ai dispositivi fissi appartenenti a tutta la rete;

- Google Workspace: account per l'accesso ai servizi della Google Workspace (@iissspantaleo.edu.it);
- Account per l'accesso alla rete wireless;
- servizio di stampa: PIN per l'utilizzo dei fotocopiatori.

**Studenti:**

- Account permette l'accesso ai dispositivi fissi appartenenti alla rete didattica;
- Google Workspace: account per l'accesso ai servizi della Google Workspace (nome.cognome@iissspantaleo.edu.it);
- Registro Elettronico: account per l'accesso al registro elettronico (NUVOLA - Madisoft)

**Genitori:**

- Registro Elettronico: account per l'accesso al registro elettronico (NUVOLA - Madisoft);
- Google Workspace del figlio, se minore: account per l'accesso ai servizi della Google Workspace (@iissspantaleo.edu.it);

Le password degli account devono essere predisposte nel rispetto delle seguenti tecniche di sicurezza:

- utilizzare il numero dei caratteri previsti dal sistema;
- non deve contenere la username come sua parte;
- non deve essere simile alla precedente;
- deve contenere almeno 8 caratteri numerici e alfabetici
- evitare di utilizzare caratteri e dati facilmente riconducibili al titolare della password (es. nome/cognome, data di nascita, hobby, nome ci persone care, ecc);
- memorizzare la password evitando supporti cartacei o digitali come promemoria;
- modificare frequentemente le password.

Ogni utente è tenuto a:

- conservare nella massima segretezza la parola di accesso;
- 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;
- effettuare la sostituzione della/e password nel caso si sospetti una perdita di segretezza della stessa.

**8 - Tutela della privacy: garanzie generali**

Tutte le operazioni relative all'uso della rete sono improntate alla tutela della privacy. Relativamente alla "tutela della persona ed altri soggetti rispetto al trattamento dei dati personali" si fa riferimento ai

Documenti disponibili sul sito ed agli Atti, predisposti dal Dirigente Scolastico, titolare del trattamento dei dati personali, in collaborazione con il Responsabile
per la Protezione dei Dati personali

**9 - 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 Dirigente Scolastico, si assume il diritto di impedire l'accesso dell'utente ai servizi informatici dell'Istituto 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.

**Diritto d'autore**

Il Diritto di autore è regolato dalla legislazione vigente sui Diritti d'Autore:

Legge del 22 aprile 1941 n° 633, modificata dalla legge 3 maggio 2019

n.37 , che all'art.70 stabilisce : "Il riassunto, la citazione o la riproduzione di brani o di parti di opera e la loro comunicazione al pubblico sono liberi se effettuati per uso di critica o di discussione, nei limiti giustificati da tali fini e purché non costituiscano concorrenza all'utilizzazione economica dell'opera; se effettuati a fini di insegnamento o di ricerca scientifica l'utilizzo deve inoltre avvenire per finalità illustrative e per fini non commerciali".

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 materiale digitali, protetti da copyright.

**10 - Norme conclusive**

Il Dirigente scolastico ha il diritto di revocare l'accessibilità temporanea o permanente ai laboratori e/o all'utilizzo di strumenti tecnologici e/o alle piattaforme di Istituto a chi non si attiene alle regole stabilite.

Il personale scolastico, gli studenti e i genitori vengono informati della pubblicazione del presente documento.

Si allega:

- Netiquette - etica e norme di buon uso dei servizi di rete

Torre del Greco (NA), 02.09.2024

Il Dirigente scolastico
*Dott. Giuseppe Mingione*
Firma autografa sostituita a mezzo stampa
ai sensi dell'art.3 c.2 D.L.vo n.39/1993