Titolo	**Acceptable Use Policy**
Tipo di documento	Procedura Operativa
Emesso da	Safeguarding Staff
Data di emissione	15/03/2025
N° Allegati	0
Stato	Attivo

Redatto	Safeguarding Staff	Safeguarding Staff
Verificato	Luca Radici	Direttore Scolastico
Approvato	Responsabile IT del gruppo e Responsabile delle operazioni relative al personale del gruppo	Responsabile IT del gruppo e Responsabile delle operazioni relative al personale del gruppo

PREMESSA

International Schools Partnership (ISP) fornisce ai dipendenti proprietà, attrezzature e sistemi per supportarli nello svolgimento dei propri ruoli e responsabilità al meglio delle loro capacità. Tutte le proprietà, le attrezzature e i sistemi forniti sono di proprietà di ISP e forniti a beneficio di ISP. Tuttavia, ISP riconosce che i dipendenti devono essere in grado di conciliare lavoro e vita personale e pertanto è felice di consentire un uso personale limitato.

Qualsiasi utilizzo, sia lavorativo che personale, deve essere appropriato, responsabile, proporzionato ed efficiente. È necessario prestare attenzione per evitare l'uso improprio delle proprietà, delle apparecchiature e dei sistemi di ISP per uso non ISP o per scopi non autorizzati poiché tali attività potrebbero essere considerate improprie e contrarie alla politica di ISP.
La nostra Politica di utilizzo accettabile stabilisce come utilizzare le proprietà, le apparecchiature e i sistemi di ISP e in che misura è consentito l'uso personale.

SICUREZZA E PASSWORD

I dipendenti sono responsabili della sicurezza dei beni e delle attrezzature loro concessi o prestati.
Computer, laptop e telefoni cellulari dovrebbero essere chiusi a chiave quando lasciati incustoditi in ufficio e non dovrebbero mai essere lasciati incustoditi in uno spazio pubblico. I dipendenti non devono consentire ad altri di accedere o utilizzare proprietà e attrezzature rilasciate o prestate loro da ISP.
Le password dovrebbero essere utilizzate su tutte le apparecchiature informatiche (IT), inclusi laptop, computer e telefoni cellulari. Le password dovrebbero essere modificate regolarmente secondo le istruzioni dell'IT e dovrebbero essere seguiti principi complessi relativi alle password.

In caso di perdita, furto, danneggiamento o violazione della sicurezza dei dati, un dipendente deve informare immediatamente il proprio diretto superiore e l'IT.

I dipendenti devono restituire qualsiasi proprietà o attrezzatura di ISP in loro possesso entro o prima del loro ultimo giorno di lavoro, a meno che non siano stati concordati accordi speciali con il proprio manager di riferimento. Dovrebbe essere consentito l'accesso a qualsiasi attrezzatura personale utilizzata per scopi lavorativi per garantire che tutto il software e/o i dati di ISP vengano opportunamente rimossi.

PRINCIPI PER L'USO DEI SISTEMI E LA SICUREZZA DEI DATI

È necessario prestare attenzione quando si aprono e-mail provenienti da fonti non richieste o quando un'e-mail appare sospetta. L'IT invierà regolarmente linee guida in tal senso, ma l'assenza di tali linee guida non esonera i dipendenti dal buon senso e dalla responsabilità personale.

Un dipendente deve informare immediatamente il proprio manager e l'IT se sospetta di aver ricevuto un virus IT e seguire le istruzioni fornite in via prioritaria.

I dipendenti non devono tentare di accedere ad aree riservate della rete o a qualsiasi informazione protetta da password, salvo quanto richiesto nell'espletamento corretto e diligente delle proprie. responsabilità. Se i dipendenti tentano di accedere a informazioni protette da password necessarie nello svolgimento dei loro compiti e non hanno già ricevuto la password, devono segnalarlo al proprio manager di riferimento.

Le informazioni e i dati non devono essere salvati o comunicati al di fuori dei sistemi ISP senza la previa autorizzazione del manager di linea e dell'IT del dipendente. Ciò include l'uso di e-mail personali, dispositivi personali e sistemi di archiviazione cloud esterni.

ETIQUETTE DELLA POSTA ELETTRONICA

È necessario osservare sempre una buona “etiquette” per la posta elettronica e le nostre linee guida e raccomandazioni per una buona etiquette per la posta elettronica sono riportate nell'Appendice.

I dipendenti non devono inviare messaggi potenzialmente offensivi, osceni, discriminatori, razzisti, molesti, prepotenti, e-mail denigratorie, diffamatorie o altrimenti inappropriate.
Chiunque ritenga di essere stato molestato, vittima di bullismo o offeso dal materiale ricevuto da un collega via e-mail deve informare il proprio responsabile o le Risorse umane. Questo principio si applica alle e-mail inviate sia da indirizzi e-mail di lavoro che personali.

I dipendenti devono evitare di dire in una e-mail qualsiasi cosa che possa causare offesa o imbarazzo o portare discredito ad ISP o a qualsiasi scuola ISP nel caso in cui l'e-mail venga inoltrata a colleghi o terze parti o diventi altrimenti di pubblico dominio. Una regola pratica sensata è presumere che gli altri possano sempre vedere ciò che è scritto: è pericolosamente facile inoltrare un'e-mail.

I dipendenti non dovrebbero:

- Inviare o inoltrare e-mail private al lavoro;
- Inviare o inoltrare catene di e-mail, e-mail spazzatura, vignette/barzellette inappropriate o pettegolezzi;
- Accettare i termini, stipulare impegni contrattuali o fare dichiarazioni tramite e-mail a meno che non sia stata ottenuta l'autorizzazione appropriata;
- Inviare messaggi dall'indirizzo e-mail di un'altra persona senza autorizzazione;
- Utilizzare il proprio indirizzo e-mail personale per inviare o ricevere e-mail per motivi di lavoro

Se un dipendente riceve una e-mail per errore, deve informare il mittente.
I dipendenti sono incoraggiati a utilizzare la propria posta elettronica personale per motivi personali, tuttavia, riconosciamo che a volte è conveniente e opportuno utilizzare la posta elettronica di lavoro, ad esempio per confermare accordi, modificare piani, registrarsi per qualcosa, ecc.

È necessario prestare la dovuta attenzione per evitare di divulgarli. informazioni riservate e per garantire che eventuali download siano sicuri e appropriati. In caso contrario verrà avviata l'apposita procedura disciplinare.
Si prevede che qualsiasi utilizzo personale dell'e-mail di lavoro (o dell'e-mail personale durante la giornata lavorativa) sarà ridotto al minimo e non sminuirà le responsabilità o le priorità lavorative.

USO DI INTERNET

Viene fornito l'accesso a Internet per consentire ai dipendenti di svolgere i propri ruoli e responsabilità. Come per la posta elettronica, è consentito un uso personale limitato. L'uso personale è un privilegio e non un diritto. Non deve essere abusato; il permesso può essere revocato o limitato in qualsiasi momento.
I dipendenti non devono accedere ad alcuna pagina web o scaricare immagini, documenti o altri file da Internet che potrebbero essere considerati illegali, offensivi, di cattivo gusto o immorali.

I dipendenti non devono pubblicare su Internet immagini fisse o in movimento di studenti o genitori, scattate durante o dopo l'orario scolastico e scattate o meno nei locali della scuola.
Come regola generale, se qualcuno potesse essere offeso dal contenuto di una pagina o se il fatto che il software di ISP abbia avuto accesso alla pagina o al file potesse essere fonte di imbarazzo se reso pubblico, la sua visualizzazione sarebbe considerata una violazione di questa politica.
I sistemi ISP non devono essere utilizzati per partecipare a chat room su Internet, pubblicare messaggi su qualsiasi forum Internet o per impostare o registrare testo o informazioni su un blog o wiki.
È necessario prestare attenzione quando si utilizzano servizi audio o di altro streaming (come radio, siti video o musicali o podcast) sul posto di lavoro affinché ciò non carichi eccessivamente e rallenti la rete di lavoro.

I dipendenti devono tenere presente che qualsiasi musica dal vivo o registrata deve essere ascoltata in privato poiché è necessaria una licenza per riprodurre musica dal vivo o registrata pubblicamente. L'uso di servizi di streaming audiovisivi per scopi non lavorativi non è appropriato durante l'orario di lavoro.
Questi principi si applicano all'uso delle apparecchiature ISP in qualsiasi momento, nonché all'uso delle apparecchiature personali durante il normale orario di lavoro.

PRINCIPI DEI SOCIAL MEDIA E DEI SERVIZI DI MESSAGGISTICA

I dipendenti sono responsabili del rispetto dei principi di ISP e devono agire in ogni momento come rappresentanti di ISP e delle nostre scuole. è quindi importante che vengano rispettati i seguenti principi:

- i dipendenti devono evitare qualsiasi comunicazione sui social media o sui servizi di messaggistica che possa causare danni gli interessi o la reputazione di ISP o delle nostre scuole;

- i social media e i servizi di messaggistica **non devono essere utilizzati** per:
    - diffamare o denigrare ISP, le nostre scuole, i nostri dipendenti o terze parti associate
    - molestare, maltrattare o discriminare illegalmente dipendenti o terzi;
    - rendere dichiarazioni false o fuorvianti; o impersonare colleghi o terzi.

- i dipendenti devono utilizzare i social media o i servizi di messaggistica per esprimere opinioni su ISP o sulle nostre scuole solo se espressamente autorizzati a farlo dal proprio superiore, a condizione che il proprio superiore ha il potere di rilasciare tale autorizzazione.

- i commenti relativi a informazioni sensibili e riservate o alla proprietà intellettuale dovrebbero non essere mai pubblicati sui social media o sui servizi di messaggistica;

- i dipendenti non devono pubblicare immagini fisse o in movimento di studenti o genitori, scattate durante o dopo l'orario scolastico, e scattate o meno nei locali della scuola, su qualsiasi sito di social media o servizio di messaggistica.

- Se un dipendente è incerto o preoccupato circa l'adeguatezza di qualsiasi dichiarazione o pubblicazione, deve astenersi dal pubblicarla finché non ne ha discusso con il proprio manager di riferimento. In tal caso si presuppone che il manager di linea chieda ulteriore consulenza, se necessario, al responsabile del brand del gruppo o al team regionale di marketing e comunicazione.

- i social media e i servizi di messaggistica non devono mai essere utilizzati in modo da violare qualsiasi altra politica di ISP. qualsiasi dipendente che violi una qualsiasi delle nostre politiche tramite i social media o il servizio di messaggistica può essere soggetto ad azioni disciplinari in linea con la procedura disciplinare locale appropriata.

- Se un dipendente vede contenuti sui social media che denigrano o riflettono negativamente ISP o una scuola, dovrebbe informare immediatamente il relativo ceo di divisione.

- A un dipendente potrebbe essere richiesto di rimuovere qualsiasi contenuto dai social media fornito da ISP o dalle nostre scuole considerando come una violazione o contraria allo spirito di questa politica.

- Tutti gli account dei social media dovrebbero essere sicuri con le massime impostazioni di privacy. I dipendenti non devono essere amici o connettersi con studenti o genitori (passati, presenti e futuri) sui social media senza previa autorizzazione del proprio amministratore delegato regionale.

- In nessun caso i dipendenti devono comunicare con gli studenti tramite i social media o servizi di messaggistica.

- Qualsiasi uso improprio dei social media o dei servizi di messaggistica deve essere segnalato al diretto superiore del dipendente o alle Risorse umane. Ove possibile e senza indebito ritardo, le prove di eventuali abusi dovrebbero essere registrate e archiviate offline in modo che possano essere affrontate adeguatamente in linea con la relativa procedura disciplinare.

- L'uso di immagini e video di bambini e studenti su qualsiasi canale digitale di ISP deve avere le autorizzazioni pertinenti di genitori o tutori, nonché altre disposizioni appropriate sulla protezione dei dati in atto che stabiliscano la base legittima su cui tali immagini vengono archiviate e condivise.

I seguenti principi si applicano sia durante che al di fuori del normale orario di lavoro e sia utilizzando la nostra attrezzatura che quella personale.

USO PERSONALE DEI SISTEMI

Come accennato, ai dipendenti può essere consentito l'uso occasionale dei sistemi Internet, di posta elettronica e telefonici di ISP per inviare e-mail personali, navigare in Internet ed effettuare telefonate personali subordinatamente a determinate condizioni stabilite di seguito:

- L'uso personale dovrebbe essere minimo, avvenire sostanzialmente al di fuori del normale orario di lavoro e non deve interferire con gli impegni lavorativi;

- L'uso personale non include l'archiviazione di documentazione personale su dispositivi o sistemi ISP a meno che ciò non sia necessario per motivi legati al lavoro (ad esempio archiviazione di una copia del passaporto per le prenotazioni di viaggi)

- L'uso personale non dovrebbe impegnare l'ISP a costi marginali;

- L'uso personale deve essere conforme alla presente politica e a qualsiasi altra politica pertinente, comprese, ma non limitate a, le nostre politiche sulla protezione dei dati, sulla dignità sul lavoro e sulla sicurezza IT.

Ci riserviamo il diritto di limitare o impedire l'accesso a determinati numeri di telefono o siti Internet se l'uso personale è eccessivo e i dipendenti devono essere consapevoli che uscendo dal loro accesso ai dispositivi e ai sistemi di ISP verrà rimosso e perderanno quindi l'accesso a qualsiasi e-mail personale inviata o ricevuti e l'accesso a qualsiasi documentazione personale conservata o archiviata.

PRINCIPI DI MONITORAGGIO

L'uso dei sistemi ISP (inclusi i sistemi telefonici e informatici e qualsiasi uso personale degli stessi) può essere continuamente monitorato da software automatizzato o in altro modo per motivi aziendali e per garantire l'adempimento delle nostre responsabilità legali come datore di lavoro. Qualsiasi monitoraggio di questo tipo viene effettuato solo nella misura consentita o come richiesto dalla legge e come necessario e giustificabile per scopi aziendali.

Ci riserviamo il diritto di recuperare il contenuto dei messaggi e-mail e/o verificare l'utilizzo di Internet (comprese le pagine visitate e le ricerche effettuate) se ragionevolmente necessario nell'interesse della nostra attività, inclusi, ma non limitati a, i seguenti scopi:

- Controllare se l'uso del sistema di posta elettronica o di internet è legittimo e conforme con questa politica;
- Per ritrovare i messaggi persi o recuperare i messaggi persi a causa di un guasto del computer;
- Supportare le indagini su presunti illeciti;

- Garantire la protezione, la sicurezza e la salvaguardia dei nostri dipendenti e studenti; oppure per ottemperare a eventuali obblighi di legge.

ALTRE POLITICHE

Qualsiasi utilizzo della posta elettronica, di Internet o di altri sistemi deve essere in linea con i requisiti e lo spirito delle nostre altre politiche, comprese, ma non limitate a, la nostra politica sulla dignità sul lavoro e le politiche e le procedure di salvaguardia.

UTILIZZO VIETATO DEI NOSTRI SISTEMI

Qualora vengano riscontrate prove di abuso, ISP può intraprendere un'indagine più approfondita in conformità con la relativa procedura disciplinare.

Si ricorda espressamente ai dipendenti che quanto segue costituisce cattiva condotta o cattiva condotta grave in linea con il Codice di condotta di ISP (si prega di notare che questo elenco non è esaustivo):

- Frode, falsificazione o altra disonestà, inclusa la fabbricazione di note spese;
- Grave violazione della riservatezza, dovuta a cattiva condotta o negligenza;
- Violenza effettiva o minacciata, o comportamento che provoca violenza;
- Danni intenzionali ai nostri edifici, impianti, proprietà o attrezzature, o alla proprietà di un allievo, dipendente, appaltatore, cliente o membro del pubblico;
- Grave uso improprio della nostra proprietà o del nostro nome (di ISP o di qualsiasi scuola);
- Accedere deliberatamente a siti Internet contenenti contenuti pornografici, illegali, offensivi, immorali o materiale osceno;
- Inosservanza ripetuta o grave delle istruzioni o qualsiasi altro grave atto di insubordinazione;
- Condotta che potrebbe portare grave discredito ad ISP o alle nostre scuole;

- Violazione della nostra politica di salvaguardia;
- Violazione della nostra politica sulla schiavitù moderna;
- Essere sotto l'effetto di alcol, droghe o altre sostanze durante l'orario di lavoro;
- Causare perdite, danni o lesioni per negligenza grave;
- Violazione grave o ripetuta delle norme in materia di salute e sicurezza o grave uso improprio delle attrezzature di sicurezza;
- Utilizzo o divulgazione non autorizzata di informazioni riservate o mancata garanzia che tali informazioni riservate sono mantenute al sicuro;
- Accettare o offrire tangenti o altri pagamenti segreti;
- Accettare un regalo superiore al valore nominale da un allievo, genitore, fornitore, appaltatore o altra terza parte in relazione al rapporto di lavoro senza il previo consenso del diretto superiore;
- Condanna per un reato che, a nostro avviso, potrebbe compromettere la nostra reputazione o il nostro rapporto con il nostro personale, i clienti o il pubblico, o influenzare in altro modo la vostra idoneità o capacità di continuare a lavorare per noi;
- Detenzione, uso, fornitura o tentata fornitura di sostanze stupefacenti
- Grave negligenza nei propri doveri o violazione grave o deliberata del contratto o dell'operatività procedure;
- Conoscere la violazione di norme legislative, statutarie o regolamentari che incidono sul proprio lavoro;
- Utilizzo, trattamento o divulgazione non autorizzati di dati personali contrari alla nostra Politica di Protezione dei Dati;
- Bullismo/molestie o discriminazioni nei confronti di dipendenti, appaltatori, alunni o genitori;
- Rifiuto di rivelare qualsiasi informazione richiesta dalla natura del rapporto di lavoro o altre informazioni che possono incidere sullo svolgimento delle attività;
- Menzogne, false dichiarazioni o occultamento deliberato di informazioni rilevanti su un CV o una domanda di lavoro;
- Fornire false informazioni su titoli di studio o diritti a lavorare allo scopo di guadagnare impiego o altri benefici;
- Divulgare informazioni false o fuorvianti ai sensi della nostra Politica di

segnalazione di irregolarità;

- Fare accuse false in malafede contro un dipendente;
- Grave utilizzo improprio dei nostri sistemi informatici (incluso download o utilizzo di software non autorizzato, utilizzo improprio di software sviluppato o concesso in licenza, utilizzo di software non autorizzato e utilizzo improprio di posta elettronica e Internet);
- Intraprendere un lavoro retribuito o non retribuito non autorizzato durante l'orario di lavoro;
- Ingresso non autorizzato in un'area vietata dell'edificio.

I dipendenti saranno tenuti a collaborare a qualsiasi indagine. Ciò include la concessione dell'accesso a Internet, siti di social media e/o servizi di messaggistica. I dipendenti devono essere consapevoli che le violazioni di questa politica possono anche costituire una violazione del loro contratto di lavoro, una violazione delle nostre procedure di tutela e una violazione del nostro Codice di Condotta.

APPENDICE – ETIQUETTE PER LE E-MAIL

Prima di inviare un'e-mail, è necessario valutare se l'e-mail è il mezzo giusto nelle circostanze rispetto a una telefonata, una conversazione faccia a faccia, una riunione, ecc. Spesso siamo inondati di e-mail e altri mezzi potrebbero essere più appropriati. Idealmente, rispondere a tutti dovrebbe essere evitata a meno che altri non traggano vantaggio dalla ricezione della risposta. Dovremmo evitare di contribuire alla congestione del sistema inviando messaggi banali, copiando o inoltrando e-mail a chi non ha bisogno di riceverle.

Le e-mail devono contenere un oggetto chiaro e breve che ne riassuma lo scopo.

I saluti dovrebbero essere appropriati per il destinatario e il suo rapporto di lavoro con il mittente. Dovrebbe essere inclusa una firma in modo che il destinatario abbia i dettagli di contatto del mittente nel caso abbia bisogno di follow- up.

È importante tenere presente che persone provenienti da culture diverse corrisponderanno in modo diverso e i messaggi dovrebbero essere adattati di conseguenza.

Occorre prestare particolare attenzione al tono e all'uso dell'umorismo. È molto facile che il tono venga frainteso senza il contesto delle espressioni facciali o vocali. I punti esclamativi in particolare contribuiscono al tono e dovrebbero essere usati con parsimonia. Allo stesso modo, anche l'umorismo può andare perduto nella traduzione, soprattutto senza il beneficio delle espressioni facciali/vocali, e c'è sempre il rischio che qualcosa che una persona ritiene divertente non venga recepito in quel modo.

Le e-mail devono essere sempre corrette prima dell'invio per verificare eventuali errori di ortografia, grammatica e/o contenuto o eventuali problemi di tono e umorismo; se qualcosa suona brusco quando viene riletto, è probabile che non arrivi bene quando viene letto dal destinatario.

Un buon consiglio è quello di aggiungere l'indirizzo e-mail del destinatario solo quando si è pronti per l'invio, in modo che un'e-mail non venga inviata troppo presto per errore ed è prudente ricontrollare che sia stato utilizzato l'indirizzo corretto (questo è particolarmente importante laddove sono dipendenti o contatti con nomi uguali o simili).