SCUOLA STATALE DI I GRADO "Italo Calvino" - PIACENZA
Sede "Don Lorenzo Milani" Via Boscarelli 23 - Piacenza - tel. 0523 711562
Sede "Angelo Genocchi" Via Stradella 51 - Piacenza - tel. 0523 480496
e-mail: pcmm00400b@istruzione.it - e-mail certificata: pcmm00400b@pec.istruzione.it
Codice Fiscale: 91061470331

POLA (PIANO ORGANIZZATIVO LAVORO AGILE) 2021
PERSONALE ATA

1. Normativa di riferimento

L'art. 10 del D. Lgs. 150/2009 non è ad oggi applicabile alla scuola; pertanto, la scuola non ha competenza ad adottare il Piano della performance e neanche il POLA, che costituisce una sezione dello stesso Piano della performance.
Tuttavia, sentite le OO.SS., si predispone il POLA quale strumento per favorire una migliore organizzazione del cosiddetto "lavoro agile".
Il POLA potrà essere rivisto sulla base di norme introdotte ai fini di contrastare la diffusione del Covid-19.

2. Attività che possono essere svolte da remoto e modalità attuative del lavoro agile

Possono essere svolte da remoto solo attività assegnate al personale amministrativo.
Possono essere svolte da remoto le seguenti attività: gestione del protocollo di comunicazioni PEO e PEC (in ingresso e in uscita), operazioni di contabilità, operazioni che comportino l'accesso a piattaforme, telefonate, achiviazione di documentazione didattica.
Non possono essere svolte da remoto le seguenti attività: consultazione di documentazione cartacea di atti depositati presso l'istituto, protocollazione di posta cartacea, gestione di pratiche riservate, controllo di materiali acquistati con fondi dell'istituto, operazioni di inventario, consegna di diplomi, consegna di attrezzature, attività indifferibili.
Nessuna unità di personale è autorizzata a portare all'esterno dell'ufficio documentazione contenente dati personali e/o sensibili.
Non possono, in ogni caso, essere svolte da remoto attività affidate a personale che necessita di affiancamento o formazione iniziale.
In caso di incertezza, sarà il dirigente scolastico, sentito il DSGA, a chiarire se una determinata attività può essere svolta in lavoro agile.

L'orario di servizio svolto in modalità agile deve essere annotato giorno per giorno dall'unità di personale su un modulo cartaceo.
Il personale in lavoro agile è tenuto a trasmettere al DSGA settimanalmente il modulo attraverso il quale ha attestato l'orario di servizio svolto.

3. Misure organizzative

Il personale interessato a svolgere servizio in modalità agile deve presentare una richiesta formale e deve essere formalmente autorizzato a svolgere il suo servizio in modalità agile.
Una unità di personale può richiedere di svolgere in lavoro agile un compito, una giornata di servizio, parte di una giornata di servizio.

Si ritiene che possa essere concesso lo smart working a condizione che questo non comprometta l'efficacia e l'efficienza del funzionamento degli uffici.
Al massimo una unità di personale può svolgere l'intero servizio in smart working. Viene data la precedenza, in ogni caso, a personale in particolari condizioni di salute, consultato, se necessario, il medico competente.
Si garantisce che le unità di personale che svolgono tutto o parte del loro servizio in smart working non subiscono penalizzazioni ai fini del riconoscimento di professionalità e della progressione di carriera.

4. Disposizioni di sicurezza. Prevenzione rischi da smart working

Raccomandazioni generali per i locali scelti per il lavoro agile:

- le attività lavorative non possono essere svolte in locali tecnici o locali non abitabili (ad es. soffitte, seminterrati, rustici, box);
- adeguata disponibilità di servizi igienici e acqua potabile e presenza di impianti a norma (elettrico, termoidraulico, ecc.) adeguatamente manutenuti;
- le superficie interne delle pareti non devono presentare tracce di condensazione permanente (muffe);
- i locali, eccettuati quelli destinati a servizi igienici, disimpegni, corridoi, vani-scala e ripostigli debbono fruire di illuminazione naturale diretta, adeguata alla destinazione d'uso e, a tale scopo, devono avere una superficie finestrata idonea;
- i locali devono essere muniti di impianti di illuminazione artificiale, generale e localizzata, atti a garantire un adeguato comfort visivo agli occupanti.

Indicazioni per l'illuminazione naturale ed artificiale:

- si raccomanda, soprattutto nei mesi estivi, di schermare le finestre (ad es. con tendaggi, appropriato utilizzo delle tapparelle, ecc.) allo scopo di evitare l'abbagliamento e limitare l'esposizione diretta alle radiazioni solari;
- l'illuminazione generale e specifica (lampade da tavolo) deve essere tale da garantire un illuminamento sufficiente e un contrasto appropriato tra lo schermo e l'ambiente circostante;
- è importante collocare le lampade in modo tale da evitare abbagliamenti diretti e/o riflessi e la proiezione di ombre che ostacolino il compito visivo mentre si svolge l'attività lavorativa.

Aerazione naturale ed artificiale:

- è opportuno garantire il ricambio dell'aria naturale o con ventilazione meccanica;
- evitare di esporsi a correnti d'aria fastidiose che colpiscano una zona circoscritta del corpo (ad es. la nuca, le gambe, ecc.);
- gli eventuali impianti di condizionamento dell'aria devono essere a norma e regolarmente manutenuti; i sistemi filtranti dell'impianto e i recipienti eventuali per la raccolta della condensa, vanno regolarmente ispezionati e puliti e, se necessario, sostituiti;
- evitare di regolare la temperatura a livelli troppo alti o troppo bassi (a seconda della stagione) rispetto alla temperatura esterna;
- evitare l'inalazione attiva e passiva del fumo di tabacco, soprattutto negli ambienti chiusi, in quanto molto pericolosa per la salute umana.

Utilizzo di smartphone e tablet

I tablet sono idonei prevalentemente alla gestione della posta elettronica e della documentazione, mentre gli smartphone sono idonei essenzialmente alla gestione della posta elettronica e alla lettura di brevi documenti. In caso di impiego di tablet e smartphone si raccomanda di:

- effettuare frequenti pause, limitando il tempo di digitazione continuata;
- evitare di utilizzare questi dispositivi per scrivere lunghi testi;
- evitare di utilizzare tali attrezzature mentre si cammina, salvo che per rispondere a chiamate vocali prediligendo l'utilizzo dell'auricolare;
- per prevenire l'affaticamento visivo, evitare attività prolungate di lettura sullo smartphone;
- effettuare periodicamente esercizi di allungamento dei muscoli della mano e del pollice (stretching)

Indicazioni per l'utilizzo sicuro dello smartphone come telefono cellulare:

- è bene utilizzare l'auricolare durante le chiamate, evitando di tenere il volume su livelli elevati.

I dispositivi potrebbero interferire con gli apparecchi acustici.
A tal fine è opportuno:

- non tenere i dispositivi nel taschino;
- in caso di utilizzo posizionarli sull'orecchio opposto rispetto a quello su cui è installato l'apparecchio acustico;
- evitare di usare il dispositivo in caso di sospetta interferenza;
- un portatore di apparecchi acustici che usasse l'auricolare collegato al telefono/smartphone potrebbe avere difficoltà nell'udire i suoni dell'ambiente circostante. Non usare l'auricolare se questo può mettere a rischio la propria e l'altrui sicurezza.

Prevenzione rischio stress da lavoro correlato
Si rinvia alle indicazioni contenute nel DVR d'Istituto.
Si ricorda che nel corrente anno scolastico è stato attivato uno sportello psicologico gratuito interno all'istituto.

4. Requisiti tecnologici

L'unità di personale in lavoro agile si avvale di strumenti informatici nella propria disponibilità o di un pc portatile concesso in comodato d'uso gratuito dall'istituto. E' necessario che il sistema operativo e gli applicativi in uso (posta elettronica, editor di testi etc.) siano aggiornati.
L'unità di personale deve ricorrere ai contratti di connettività alla rete Internet di cui dispone per fini personali.
L'unità di personale in lavoro agile deve conoscere il Vademecum predisposto dall'AgID per lavorare online in sicurezza.

5. Percorsi formativi del personale, anche dirigenziale

Le attività formative vengono svolte di norma a distanza.
Al personale sono trasmesse note scritte utili alla gestione di procedure specifiche.
Viene proposto un percorso di n. 2 ore di formazione sulla Privacy.
A tutto il personale amministrativo viene offerta la possibilità di seguire il modulo ECDL relativo alla IC security.
Si favorisce la partecipazione a webinar in orario di servizio.

Vengono trasmesse le seguenti buone prassi di sicurezza:

BUONE PRASSI DI SICUREZZA (**Da:** noreply@istruzione.it <noreply@istruzione.it> **Inviato:** 18 febbraio 2021 18:17 **Oggetto:** CSIRT MI - Raccomandazioni e Indicazioni per la Sicurezza 18/02/2021)

Si ribadisce (...) di:

- scansionare periodicamente per la ricerca virus le postazioni di lavoro ed i dispositivi utilizzati per lavoro;
- nel caso di utilizzo del PC personale (telelavoro/smart working) assicurarsi periodicamente:

- che il sistema operativo sia aggiornato;
- che la propria postazione di lavoro sia dotata di antivirus e che questo sia aggiornato per una periodica scansione;
- che le proprie password di posta e strumenti di lavoro siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che, al momento della modifica, non siano apportate solo piccole modifiche (come ad esempio numerazioni progressive...).

- non usare l'account di lavoro per registrarsi in internet per fini non riconducibili alla sfera di lavoro ed evitare di salvare le password nel browser di navigazione internet;
- si consiglia di non lasciare il PC portatile incustodito;
- si raccomanda l'uso di supporti removibili quali chiavette usb e/o hard disk esterni ecc. con molta cautela. Al momento della connessione di un supporto removibile, si consiglia di avviare una scansione completa dello stesso attraverso il software antivirus.

Qualora doveste incorrere in messaggi mail di phishing, si ricorda quanto segue.

- non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungano da caselle non note;
- non installare software sulle proprie postazioni di lavoro, soprattutto se a seguito di sollecitazioni via e-mail;
- non dare seguito alle richieste incluse nei messaggi;
- nel caso in cui le richieste provengano da parte del personale tecnico dell'Amministrazione, verificare attentamente il contesto: *l'e-mail era attesa? Le frasi sono scritte con grammatica corretta? Il software da installare ha un fine specifico? Eventuali link nell'e-mail puntano a siti conosciuti? Il mittente è corretto?*

Si ricorda inoltre che nell'area riservata intranet allo CSIRT MI (dopo il login, sezione: *Area Riservata > Computer Security Incident Response Team > Security Awareness*) sono presenti i contenuti relativi a campagne malevole di phishing in corso ed aggiornamenti su nuovi virus che potrebbero infettare le postazioni di lavoro del personale della Pubblica Amministrazione.
E' fortemente consigliata la lettura dei suddetti contenuti, allo scopo di tenersi aggiornati sui rischi informatici incombenti sull'Amministrazione e proteggere sia la propria operatività sia il patrimonio informativo del Ministero da possibili attacchi.

CSIRT-MI

Raccomandazioni di sicurezza per l'Utente

(smart working)

Si fa raccomandazione agli Utenti, per quanto concerne il proprio PC di casa usato in telelavoro, di assicurarsi periodicamente:

1. che il sistema operativo della propria workstation sia aggiornato;
2. che la propria workstation sia dotata di antivirus e che questo sia aggiornato;
3. che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che afferiscono a sfera lavorativa e personale.
Al momento della modifica delle password evitare di fare solo piccole modifiche come ad esempio numerazioni progressive ecc…;
4. di eseguire il backup periodico dei dati elaborati sul proprio PC nell'ambito della sfera lavorativa;

Si consiglia inoltra di evitare di iscriversi a siti internet non riconducibili alla sfera lavorativa, ovvero utilizzando la casella di posta istituzionale; tali siti potrebbero infatti essere poco sicuri nella

protezione dei dati personali, con eventuali ripercussioni in violazioni all'interno della propria operatività lavorativa.

CSIRT-MI
Raccomandazioni di sicurezza per l'Utente

Allo scopo di limitare l'occorrenza di incidenti di sicurezza si rappresentano le seguenti raccomandazioni.

- non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungono da caselle di posta non note;
- non installare software sulla propria postazione di lavoro gestita, soprattutto se a seguito di sollecitazioni via e-mail che presentino link di accesso ad altre pagine o di esecuzione file.
- non dare seguito alle richieste di e-mail sospette;
- nel caso in cui la richiesta provenga da parte del personale tecnico della nostra Amministrazione, verificare attentamente il contesto: ovvero se l'e-mail fosse attesa, le frasi siano scritte con grammatica e sintassi corretta, se il software di cui si richiede l'installazione abbia un fine specifico, se eventuali link nell'email puntino a siti conosciuti, se il mittente fosse noto e/o corretto.

In caso di dubbi rispetto a quanto sopra rivolgersi sempre conferma ai rispettivi referenti informatici.

6. Gli strumenti di rilevazione e di verifica periodica dei risultati conseguiti, anche in termini di miglioramento dell'efficacia e dell'efficienza dell'azione amministrativa, della digitalizzazione dei processi, nonché della qualità dei servizi erogati, anche coinvolgendo i cittadini, sia individualmente, sia nelle loro forme associative

In sede di rendicontazione sociale si valuteranno i risultati conseguiti rispetto al territorio.

Il Dirigente Scolastico
Elisabetta Ghiretti
(firma autografa sostituita a mezzo stampa ai sensi
e per gli effetti dell'art.3 c.2 del D.Lgs. 39/93)