Azienda Ospedaliera di Perugia

Azienda Ospedaliera di Perugia

Direzione - Sede legale: Ospedale Santa Maria della Misericordia di Perugia
Piazzale Giorgio Menghini 8/9 – Sant'Andrea delle Fratte – 06129 PERUGIA
Partita IVA/ CF 02101050546 – TEL. 075.5781
PEC aosp.perugia@postacert.umbria.it SITO WEB www.ospedale.perugia.it

Regolamento in materia di lavoro agile (*smart working*)
ai sensi del CCNL Comparto Sanità 2019-2021.

INDICE

Premessa
Nozione e finalità

Con Decreto dell'8 ottobre 2021 *"Modalità organizzative per il rientro in presenza dei lavoratori delle pubbliche amministrazioni"* (pubblicato in Gazzetta Ufficiale il 13 ottobre 2021), il Ministro della pubblica amministrazione, in attuazione delle disposizioni impartite con Decreto della Presidenza del Consiglio dei ministri del 23 settembre 2021, ha previsto che il lavoro agile non è più una modalità ordinaria di svolgimento della prestazione lavorativa, superando, pertanto, le disposizioni adottate in materia per far fronte alla fase emergenziale pandemica da Sars-Cov-2, cessata il 31 marzo 2022 (D.L. 24 marzo 2022).

Ad oggi, la disciplina di riferimento del lavoro agile o *smart working* è contenuta nella Legge 22 maggio 2017, n. 81 (articoli 18-24), come da ultimo modificata dalla Legge 4 agosto 2022, n. 122 (che ha convertito con modificazioni il D.L. 21 giugno 2022, n. 73, c.d. Decreto Semplificazioni) e nel CCNL Comparto Sanità 2019-2021, sottoscritto il 02/11/2022 (articoli 76-80), secondo cui il lavoro agile è una modalità di esecuzione della prestazione mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa.

La prestazione lavorativa viene eseguita in parte all'interno dei locali aziendali e in parte all'esterno, senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale derivanti dalla legge e dalla contrattazione collettiva.

Tale particolare modalità di esecuzione della prestazione di lavoro subordinato è stata introdotta al fine di incrementare la competitività e di agevolare la conciliazione dei tempi di vita e lavoro.

Art. 1
Attivitá eseguibili in modalità agile

1. L'esecuzione della prestazione in modalità agile è realizzabile quando attività e funzioni siano almeno in parte delocalizzabili, cioè tali da non richiedere la costante presenza fisica nella sede di lavoro del dipendente addetto. A titolo meramente esemplificativo si riporta un'elencazione di tipologie di attività che, di norma, possono essere svolte in modalità agile*:*

    a) analisi, studio, ricerca e stesura di testi e relazioni connesse con i compiti d'ufficio;
    b) attività di approfondimento normativo o giurisprudenziale;
    c) predisposizione di atti/provvedimenti o di minute degli stessi, di relazioni propedeutiche, ovvero di modulistica, ovvero di documentazione tecnica;
    d) elaborazione/inserimento dati, monitoraggio, reportistica;
    e) utilizzo di appositi sistemi applicativi per lo svolgimento delle attività/funzioni attribuite in base alle competenze delle strutture.

2. Ai sensi dell'art. 77, comma 2 del CCNL 2019/2021, è escluso dall'accesso alla modalità di lavoro agile il personale adibito a mansioni che prevedono la necessaria presenza del lavoratore presso l'Azienda Ospedaliera di Perugia.

3. Tra le attività che richiedono la presenza del lavoratore presso la sede, si evidenziano:
   - prestazioni che si svolgono tramite diretto contatto con l'utenza, tra cui, a titolo esemplificativo e non esaustivo:
     - assistenza medico-sanitaria con necessaria presenza dell'utente;
     - prestazioni socio-sanitarie;
     - sportelli di front-office.

   - prestazioni di presidio di sedi aziendali, tra cui, a titolo esemplificativo e non esaustivo:
     - portineria;
     - ricezione di posta/documenti/bolle di trasporto.

   - prestazioni che comportano attività manuali correlate all'ambiente di lavoro, tra cui, a titolo esemplificativo e non esaustivo:
     - prestazioni tecniche per attività da imbianchino, muratore ecc.;
     - attività di magazzino;
     - servizi tecnico-economali.

4. Eventuali ulteriori attività potranno essere di volta in volta valutate dal responsabile in ragione delle specifiche funzioni attribuite alla struttura di assegnazione del dipendente in sede di sottoscrizione dell'accordo individuale.

Art. 2
Prioritá di accesso al lavoro agile

1. L'art. 18, comma 3 bis, della Legge 22 maggio 2017, n. 81, come modificato dall'art. 4, comma 1, lett. b) del D.Lgs. 30 giugno 2022, n. 105, stabilisce che i datori di lavoro che stipulano accordi per l'esecuzione della prestazione di lavoro in modalità agile sono tenuti in ogni caso a riconoscere priorità alle richieste di esecuzione del rapporto di lavoro in modalità agile formulate:

   - dalle lavoratrici e dai lavoratori con figli fino a dodici anni di età o senza alcun limite di età nel caso di figli in condizioni di disabilità ai sensi dell'articolo 3, comma 3, della legge 5 febbraio 1992, n. 104;

   - dei lavoratori con disabilità in situazione di gravità accertata ai sensi dell'articolo 4, comma 1, della legge 5 febbraio 1992, n. 104;

   - *caregivers* ai sensi dell'articolo 1, comma 255, della legge 27 dicembre 2017, n. 205.

2. L'art. 1, comma 306 della Legge n. 197 del 29 dicembre 2022 stabilisce che: "*Fino al 31 marzo 2023, per i lavoratori dipendenti pubblici e privati affetti dalle patologie e condizioni individuate dal decreto del Ministro della salute di cui all'articolo 17, comma 2, del decreto-legge 24 dicembre 2021, n. 221, convertito, con modificazioni, dalla legge 18 febbraio 2022, n. 11, il datore di lavoro assicura lo svolgimento della prestazione lavorativa in modalità agile anche attraverso l'adibizione a diversa mansione compresa nella medesima categoria o area di inquadramento, come definite dai contratti collettivi di lavoro vigenti, senza alcuna decurtazione*

della retribuzione in godimento. Resta ferma l'applicazione delle disposizioni dei relativi contratti collettivi nazionali di lavoro, ove più favorevoli".

Art. 3
Attivazione del lavoro agile

1. L'attivazione del lavoro agile avviene mediante compilazione dell'accordo individuale utilizzando esclusivamente il modello allegato al presente Regolamento (Allegato A) redatto in conformità a quanto previsto dal "*Protocollo nazionale sul lavoro in modalità agile"* sottoscritto il 7 dicembre 2021, a seguito dell'accordo tra il Ministero del Lavoro e delle Politiche Sociali e le Parti sociali, ed altresì nel rispetto di quanto stabilito nella sezione dedicata all'interno del PIAO Aziendale.

2. La sottoscrizione dell'accordo di cui al comma 1 da parte del Dirigente, previo nulla osta del Direttore Amministrativo, equivale all'autorizzazione allo svolgimento dell'attività in lavoro agile. Successivamente il Dirigente/Responsabile:
   - comunica ai Sistemi Informativi Aziendali l'attivazione del lavoro agile per il dipendente interessato ai fini dell'abilitazione dello stesso all'accesso dall'esterno alla rete aziendale;
   - trasmette l'accordo individuale protocollato alla Direzione Personale che, entro e non oltre i 5 giorni lavorativi successivi, assolverà agli obblighi di comunicazione e assicurazione obbligatoria di cui all'art. 23 Legge 22 maggio 2017, n. 81.

3. Non saranno accettate domande e/o accordi individuali redatti con modulistica diversa da quella allegata e/o presentati con modalità diverse da quelle indicate nel presente Regolamento.

4. Il personale eventualmente già in *smart working* con modalità semplificata ai sensi della disciplina emergenziale previgente ha l'obbligo di adeguarsi alle condizioni e modalità previste dal presente Regolamento, con conseguente necessità di procedere a sottoscrizione di nuovo accordo.

Art. 4
Accordo individuale

1. L'accordo individuale di lavoro agile è stipulato per iscritto ai fini della regolarità amministrativa e della prova ed è sottoscritto dal dipendente interessato, dal Dirigente/Responsabile della struttura di appartenenza e dal Direttore Amministrativo.

2. L'accordo individuale è conservato presso la S.C. Direzione Personale per un periodo di cinque anni dalla sottoscrizione e verrà inserito nel fascicolo del dipendente.

3. Nell'accordo individuale di lavoro agile sono definiti i seguenti elementi:

   a) <u>LUOGO</u>

I luoghi di esecuzione del lavoro in modalità agile devono essere idonei a garantire adeguati livelli di privacy, salute e sicurezza.

b) DURATA E ARTICOLAZIONE

L'accordo è a tempo determinato per la durata massima di un anno, rinnovabile.

La programmazione delle giornate di lavoro agile è definita dal Dirigente/Responsabile di riferimento, su base settimanale o mensile, tenendo conto delle esigenze del dipendente e compatibilmente con quelle organizzative della Struttura di appartenenza.

L'accordo deve prevedere una specifica indicazione della data di inizio e fine dello stesso nonché delle giornate di lavoro da svolgere in sede e di quelle da svolgere a distanza.

La prestazione con modalità di lavoro agile avviene, di norma, entro i limiti di seguito descritti:

- 2 giornate la settimana per il personale in possesso dei requisiti di priorità di accesso al lavoro agile;
- 1 giornata la settimana per il restante personale.
- altra articolazione: n. …… giornate a settimana

(*al riguardo si rinvia alle disposizioni vigenti relative ai lavoratori fragili di cui all'art. 1, comma 306 della L. 29/12/2022, n. 197 e s. m. e i.*)**.**

Ferma restando la possibilità per le parti di concordare diverse articolazioni in ragione di particolari esigenze personali e organizzative.

Laddove la data di inizio indicata nell'accordo individuale sia anteriore alla data di sottoscrizione del Direttore Amministrativo, l'attivazione del lavoro agile decorrerà da quest'ultima.

c) DOTAZIONE TECNOLOGICA

La prestazione lavorativa in modalità agile è svolta mediante utilizzo di supporti informatici di norma forniti dall'amministrazione. In caso di indisponibilità, la dotazione informatica è a carico del dipendente.

In ogni caso il dipendente è tenuto ad accertare la presenza delle condizioni che garantiscono le condizioni minime di tutela della salute e sicurezza del lavoratore nonché la piena operatività della dotazione informatica e ad adottare tutte le precauzioni e le misure necessarie e idonee a garantire la più assoluta riservatezza sui dati e sulle informazioni in possesso dell'Ente che vengono trattate dal lavoratore stesso.

Al fine di garantire le comunicazioni, nelle giornate di lavoro in modalità agile il dipendente è tenuto rendersi reperibile, anche attivando la deviazione della chiamata dal numero della postazione d'ufficio al cellulare di servizio o personale.

I consumi elettrici, di connessione alla rete Internet, quelli relativi alle comunicazioni telefoniche per ragioni d'ufficio e quant'altro necessario sono a carico del dipendente.

d) MODALITÀ E TEMPI DI ESECUZIONE DELLA PRESTAZIONE

L'accordo individuale deve indicare le attività da svolgere e gli obiettivi generali da perseguire.

La prestazione lavorativa in modalità agile è svolta nel rispetto dei limiti di durata massima dell'orario di lavoro giornaliero e settimanale derivanti dalla legge e dalle norme della contrattazione collettiva, non può generare lavoro straordinario ed è organizzata nel rispetto dei criteri sottoindicati.

La fascia oraria di contattabilità non può superare l'orario medio giornaliero di lavoro del dipendente e deve essere determinata nell'accordo individuale.

È prevista una fascia di inoperabilità nella quale il lavoratore non può erogare alcuna prestazione lavorativa. Tale fascia comprende il periodo di 11 ore di riposo consecutivo a cui il lavoratore è tenuto nonché il periodo di lavoro notturno tra le ore 22:00 e le ore 06:00 del giorno successivo.

Il regime giuridico derivante dal contratto e relativo a ferie, malattie, aspettative, permessi (giornalieri ed orari) rimane inalterato. Per effetto della distribuzione discrezionale del tempo di lavoro, non sono

configurabili, invece, prestazioni straordinarie, trasferte, lavoro disagiato, lavoro svolto in condizioni di rischio.
In caso di problematiche di natura tecnica e/o informatica, e comunque in ogni caso di cattivo funzionamento dei sistemi informatici, qualora lo svolgimento dell'attività lavorativa a distanza sia impedito o sensibilmente rallentato, il dipendente è tenuto a darne tempestiva informazione al proprio dirigente. Questi, qualora le suddette problematiche dovessero rendere temporaneamente impossibile o non sicura la prestazione lavorativa, può richiamare il dipendente a lavorare in presenza. In caso di ripresa del lavoro in presenza, il lavoratore è tenuto a completare la propria prestazione lavorativa fino al termine del proprio orario ordinario di lavoro.
Per sopravvenute esigenze di servizio il dipendente in lavoro agile può essere richiamato in sede, con comunicazione che deve pervenire in tempo utile per la ripresa del servizio e, comunque, almeno il giorno prima. Il rientro in servizio non comporta il diritto al recupero delle giornate di lavoro agile non fruite.
Il lavoratore ha diritto alla disconnessione. A tal fine, ferma restando la fascia di inoperabilità, negli orari diversi da quelli ricompresi nella fascia di contattabilità non sono richiesti contatti con i colleghi o con il dirigente per lo svolgimento della prestazione lavorativa, la lettura delle email, la risposta alle telefonate e ai messaggi, l'accesso e la connessione al sistema informativo dell'Azienda o Ente.
Il buono pasto, sostitutivo del servizio mensa, non è dovuto per le giornate di lavoro agile.

e) CONTROLLO DELLA PRESTAZIONE LAVORATIVA

Per poter rendicontare digitalmente le giornate lavorate in modalità agile, il dipendente deve accedere al Self Service ed inserire un nuovo giustificativo scegliendo la causale *"Smart Working".* Nel campo "Note" è, inoltre, necessario descrivere sinteticamente il lavoro svolto.
Ciascun Responsabile, al momento dell'autorizzazione della richiesta del giustificativo in questione, deve controllare quanto dichiarato dal dipendente al fine di monitorare costantemente l'espletamento delle attività assegnate.

f) RECESSO

In presenza di un giustificato motivo, ciascuno dei contraenti può recedere prima della scadenza del termine con preavviso non inferiore a trenta giorni.
Nel caso di lavoratori disabili ai sensi dell'articolo 1 della legge 12 marzo 1999, n. 68, il termine di preavviso del recesso da parte del datore di lavoro non può essere inferiore a novanta giorni, al fine di consentire un'adeguata riorganizzazione dei percorsi di lavoro rispetto alle esigenze di vita e di cura del lavoratore.
Costituisce giustificato motivo per l'Azienda il venir meno della compatibilità organizzativa della prestazione resa in modalità agile, l'ingiustificato rispetto delle attività assegnate al dipendente e/o dei tempi di esecuzione delle stesse, il mancato rispetto o venir meno delle condizioni di idoneità dei luoghi di espletamento delle attività in modalità agile, il mancato rispetto delle fasce di contattabilità, ed ogni altra condotta da cui possa derivare la violazione degli obblighi di diligenza e riservatezza.

g) OBBLIGHI DI DILIGENZA E RISERVATEZZA

Il dipendente (*smart worker*) è tenuto ad attenersi alle istruzioni ricevute dal dirigente relativamente all'esecuzione del lavoro in modalità agile e, in particolare, per l'assolvimento dei compiti assegnati. Inoltre, è tenuto a rispettare i seguenti obblighi di condotta, la cui violazione può dar luogo all'applicazione di sanzioni disciplinari:

- utilizzare i dati trattati in modo lecito, solo per gli scopi specificati dal dirigente e per le finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- assicurare l'assoluta riservatezza/segretezza delle informazioni trattate, elaborate e contenute in banche dati cui abbia l'accesso;
- rispettare il divieto di comunicazione e/o diffusione dei dati trattati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate dal dirigente;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze riferite a compiti istituzionali;
- verificare sempre ed in caso di interruzione del lavoro, anche temporanea, che i dati trattati non siano accessibili a terzi non autorizzati;
- informare il dirigente in caso di eventi di sicurezza informatica che coinvolgano i dati trattati;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli e/o nei supporti informatici, avendo cura che l'accesso ad essi sia consentito esclusivamente ai soggetti autorizzati;
- rispettare le misure di prevenzione e protezione previste dalla normativa vigente in materia di tutela della salute e sicurezza nei luoghi di lavoro;
- rispettare la normativa vigente in materia di tutela della privacy e di sicurezza dei dati.

Il lavoratore si impegna a rispettare le prescrizioni indicate nelle informative sulla salute e sicurezza sul lavoro agile, sulla sicurezza informatica e sul trattamento dei dati fornite dall’Azienda e allegate al contratto individuale.

ALLEGATO A

ACCORDO INDIVIDUALE

LAVORO AGILE (*SMART WORKING*)

La/Il Dirigente Responsabile_____ della struttura _____

La/Il lavoratrice/lavoratore _____, matricola,_____

CF_____

CONVENGONO

- ☐ di svolgere la prestazione lavorativa in modalità agile all'esterno dei locali dell'Azienda Ospedaliera di Perugia per n. 2 giornate a settimana, in quanto_____;

- ☐ di svolgere la prestazione lavorativa in modalità agile all'esterno dei locali dell'Azienda Ospedaliera di Perugia per n. 1 giornata a settimana, in quanto_____;

- ☐ di svolgere la prestazione lavorativa in modalità agile all'esterno dei locali dell'Azienda Ospedaliera di Perugia per n. _____ giornate a settimana, in quanto lavoratore fragile o altro_____;

nei termini ed alle condizioni di seguito indicate.

1. Luogo

I luoghi di esecuzione del lavoro in modalità agile devono essere idonei a garantire adeguati livelli di privacy, salute e sicurezza.

2. Durata

Il presente accordo individuale a termine produce effetti dal _____fino al_____.

Il lavoro sarà svolto in modalità agile nelle specifiche giornate di _____.

Nelle restanti giornate il lavoro sarà svolto in sede.

Al termine del periodo sopra indicato verrà ripristinata, senza necessità di alcuna comunicazione preventiva, l’ordinaria modalità della prestazione di lavoro, salvo il rinnovo del presente accordo.

3. Dotazione tecnologica

- ☐ di utilizzare la dotazione tecnologica aziendale.

- ☐ di utilizzare la propria dotazione tecnologica e di garantirne adeguata cura, conservazione e uso esclusivo in ambito domestico.

In ogni caso il dipendente è tenuto ad accertare la presenza delle condizioni che garantiscono le condizioni minime di tutela della salute e sicurezza del lavoratore nonché la piena operatività della dotazione informatica e ad adottare tutte le precauzioni e le misure necessarie e idonee a garantire la più assoluta riservatezza sui dati e sulle informazioni in possesso dell'Ente che vengono trattate dal lavoratore stesso.
Al fine di garantire le comunicazioni, nelle giornate di lavoro in modalità agile il dipendente è tenuto rendersi reperibile, anche attivando la deviazione della chiamata dal numero della postazione d'ufficio al cellulare di servizio o personale.
I consumi elettrici, di connessione alla rete Internet, quelli relativi alle comunicazioni telefoniche per ragioni d'ufficio e quant'altro necessario sono a carico del dipendente.

4. Attività da svolgere in modalità agile ed obiettivi

Nel seguito si predeterminano gli obiettivi e le modalità di verifica.

Attività	Modalità di verifica

5. Modalità e tempi di esecuzione della prestazione – diritto alla disconnessione

La prestazione lavorativa in modalità agile è svolta nel rispetto dei limiti di durata massima dell'orario di lavoro giornaliero e settimanale derivanti dalla legge e dalle norme della contrattazione collettiva, non può generare lavoro straordinario ed è organizzata nel rispetto dei criteri sottoindicati.
La fascia oraria di contattabilità è compresa dalle_____ alle_____.
È prevista una fascia di inoperabilità nella quale il lavoratore non può erogare alcuna prestazione lavorativa. Tale fascia comprende il periodo di 11 ore di riposo consecutivo a cui il lavoratore è tenuto nonché il periodo di lavoro notturno tra le ore 22:00 e le ore 06:00 del giorno successivo.
Il regime giuridico derivante dal contratto e relativo a ferie, malattie, aspettative, permessi (giornalieri ed orari) rimane inalterato. Per effetto della distribuzione discrezionale del tempo di lavoro, non sono configurabili, invece, prestazioni straordinarie, trasferte, lavoro disagiato, lavoro svolto in condizioni di rischio.
Il lavoratore ha diritto alla disconnessione. A tal fine, ferma restando la fascia di inoperabilità, negli orari diversi da quelli ricompresi nella fascia di contattabilità non sono richiesti contatti con i colleghi o con il dirigente per lo svolgimento della prestazione lavorativa, la lettura delle email, la risposta alle telefonate e ai messaggi, l'accesso e la connessione al sistema informativo dell'Azienda o Ente.
Il buono pasto, sostitutivo del servizio mensa, non è dovuto per le giornate di lavoro agile.

6. Presenza in sede

In caso di problematiche di natura tecnica e/o informatica, e comunque in ogni caso di cattivo funzionamento dei sistemi informatici, qualora lo svolgimento dell'attività lavorativa a distanza sia impedito o sensibilmente rallentato, il dipendente è tenuto a darne tempestiva informazione al proprio dirigente. Questi, qualora le suddette problematiche dovessero rendere temporaneamente impossibile o non sicura la prestazione lavorativa, può richiamare il dipendente a lavorare in presenza. In caso di ripresa del lavoro in presenza, il lavoratore è tenuto a completare la propria prestazione lavorativa fino al termine del proprio orario ordinario di lavoro.

Per sopravvenute esigenze di servizio il dipendente in lavoro agile può essere richiamato in sede, con comunicazione che deve pervenire in tempo utile per la ripresa del servizio e, comunque, almeno il giorno prima. Il rientro in servizio non comporta il diritto al recupero delle giornate di lavoro agile non fruite.

7. Recesso

In presenza di un giustificato motivo, ciascuno dei contraenti può recedere prima della scadenza del termine con preavviso non inferiore a trenta giorni.

Nel caso di lavoratori disabili ai sensi dell'articolo 1 della legge 12 marzo 1999, n. 68, il termine di preavviso del recesso da parte del datore di lavoro non può essere inferiore a novanta giorni, al fine di consentire un'adeguata riorganizzazione dei percorsi di lavoro rispetto alle esigenze di vita e di cura del lavoratore.

Costituisce giustificato motivo per l'Azienda il venir meno della compatibilità organizzativa della prestazione resa in modalità agile, l'ingiustificato rispetto delle attività assegnate al dipendente e/o dei tempi di esecuzione delle stesse, il mancato rispetto o venir meno delle condizioni di idoneità dei luoghi di espletamento delle attività in modalità agile, il mancato rispetto delle fasce di contattabilità, ed ogni altra condotta da cui possa derivare la violazione degli obblighi di diligenza e riservatezza.

8. Obblighi del dipendente

Il dipendente (*smart worker*) è tenuto ad attenersi alle istruzioni ricevute dal dirigente relativamente all'esecuzione del lavoro in modalità agile e, in particolare, per l'assolvimento dei compiti assegnati. Inoltre, è tenuto a rispettare i seguenti obblighi di condotta, la cui violazione può dar luogo all'applicazione di sanzioni disciplinari:

• utilizzare i dati trattati in modo lecito, solo per gli scopi specificati dal dirigente e per le finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;

• assicurare l'assoluta riservatezza/segretezza delle informazioni trattate, elaborate e contenute in banche dati cui abbia l'accesso;

• rispettare il divieto di comunicazione e/o diffusione dei dati trattati;

• segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate dal dirigente;

• accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze riferite a compiti istituzionali;

• verificare sempre ed in caso di interruzione del lavoro, anche temporanea, che i dati trattati non siano accessibili a terzi non autorizzati;

• informare il dirigente in caso di eventi di sicurezza informatica che coinvolgano i dati trattati;

• raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli e/o nei supporti informatici, avendo cura che l'accesso ad essi sia consentito esclusivamente ai soggetti autorizzati;

• rispettare le misure di prevenzione e protezione previste dalla normativa vigente in materia di tutela della salute e sicurezza nei luoghi di lavoro;

• rispettare la normativa vigente in materia di tutela della privacy e di sicurezza dei dati.

Il lavoratore si impegna a rispettare le prescrizioni indicate nelle informative sulla salute e sicurezza sul lavoro agile, sulla sicurezza informatica e sul trattamento dei dati fornite dall'Azienda e allegate al presente contratto individuale.

Luogo e data _____

Firma della/del lavoratrice/lavoratore

Firma della/del Dirigente Responsabile

Firma del Direttore Amministrativo

ALLEGATO B

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI
ai sensi degli artt. 13 e 14 del Regolamento UE 679/2016 e del D.Lgs.196/2003 e ss.mm.ii.

— LAVORO AGILE / SMART WORKING —

L'Azienda Ospedaliera di Perugia con sede legale: Ospedale Santa Maria della Misericordia di Perugia, Piazzale Giorgio Menghini 8/9 – Sant'Andrea delle Fratte – 06129 PERUGIA, Partita IVA/ CF 02101050546 – TEL. 075.5781 PEC aosp.perugia@postacert.umbria.it SITO WEB www.ospedale.perugia.it in qualità di Titolare del trattamento (di seguito "Titolare''), tratterà i Suoi dati personali.	Chi tratta i miei dati?
I dati personali saranno raccolti e trattati, sia con strumenti informatici, sia in modalità analogica, esclusivamente per i conseguenti adempimenti attinenti allo svolgimento della prestazione lavorativa, al fine di assicurare altresì il regolare svolgimento e la continuità delle attività istituzionali. Tutto questo nel pieno rispetto del segreto professionale e d'ufficio e dei principi di liceità, sicurezza, correttezza, riservatezza, trasparenza, limitazione delle finalità e minimizzazione dei dati. La disponibilità, la gestione, l'accesso, la conservazione e la fruibilità dei dati è garantita dall'adozione di misure tecniche ed organizzative concordate con il Titolare. Il trattamento dei dati rientra nell'ambito dell'attività lavorativa complessivamente svolta in modalità "AGILE" da remoto, autorizzata previo accordo individuale, e delle funzioni svolte, in costanza dell'espletamento dell'incarico attribuito e relativi ai Settori/Uffici/ Aree di riferimento.	Natura e Finalità del trattamento dei dati
I dati vengono trattati ai sensi dell'art. 6 comma 1 lett. b) del Regolamento UE 679/2016, della Legge 22 maggio 2017, n. 81, del CCNL Comparto Sanità 2019-2021, sottoscritto il 02/11/2022 e dall'art. 1, comma 306, Legge 197/2022.	Base Giuridica
I dati personali saranno trattati in modalità informatica e in modalità analogica, secondo quanto previsto dalla normativa vigente e nel rispetto delle misure di sicurezza. Non è previsto il trasferimento dei dati in un paese terzo.	Modalità del Trattamento dati
Il Titolare, nei soli casi previsti dalla legge, potrà comunicare i dati trattati, a soggetti pubblici che agiscono in qualità di autonomi Titolari o Contitolari del trattamento (esempio: autorità giudiziaria, istituti previdenziali, assistenziali e di assicurazione contro gli infortuni sul lavoro, Regione, Ministeri, ecc.) ed a soggetti privati in rapporto contrattuale, nominati Responsabili del trattamento ai sensi dell'art. 28 del sopracitato Regolamento (gestori e manutentori di piattaforme informatiche, ecc.), ai quali sono demandate operazioni di trattamento per lo svolgimento delle attività correlate al perseguimento delle suddette finalità.	Destinatari o Categorie dei Destinatari
I dati personali saranno trattati e conservati per il periodo dell'attività lavorativa complessivamente svolta in modalità "AGILE" da remoto, fatto salvo il maggior tempo necessario per adempiere agli obblighi di legge in ragione della natura del dato o per motivi di interesse pubblico o per l'esercizio di pubblici poteri. Esaurite tutte le finalità che legittimano la conservazione dei dati, il Titolare avrà cura di cancellarli.	Periodo di Conservazione
Le categorie di dati personali che possono essere trattate nella gestione del processo/procedimento/attività sono: - tutti i dati inerenti la gestione del rapporto di lavoro, già oggetto di comunicazione; - dati idonei a rilevare la posizione "dati di geolocalizzazione" (eventuali); - nominativo, indirizzo o altri elementi di identificazione personale (es. posta elettronica).	Categorie di dati personali trattate

L'interessato ha il diritto di ottenere dal Titolare, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento UE 679/2016). Ha diritto, altresì, a non essere sottoposto a processo decisionale automatizzato, compresa la profilazione e, qualora il trattamento sia basato sul consenso, di revocare il consenso in qualsiasi momento senza pregiudicare la liceità basata prima della revoca. L'interessato ha inoltre il diritto di presentare reclamo all'Autorità Garante per la protezione dei dati personali, se ritiene che il trattamento dei suoi dati personali sia effettuato in violazione di legge.	Diritti dell'Interessato
Se ha dei dubbi, se conserviamo dati errati, incompleti o se pensa che abbiamo gestito male i Suoi dati, La preghiamo di contattare il Titolare o il Responsabile della Protezione dei Dati (RPD/DPO) all'indirizzo email dpo@ospedale.perugia.it	A chi mi posso rivolgere?
L'Informativa è lo strumento previsto dal Regolamento UE 679/2016 per applicare il principio di trasparenza e agevolare l'interessato nella gestione delle informazioni che lo riguardano. Al variare delle modalità di trattamento e/o della normativa, la presente potrà essere revisionata/integrata.	Aggiornamenti

ALLEGATO C

Istruzioni Operative: Lavoro agile – politiche di sicurezza sul corretto utilizzo dei dispositivi mobili

Redatto da	Referente Gruppo di lavoro		
		Firma	*data*
Verificato da	Responsabile Sistemi Informatici e Transizione all'Amministrazione Digitale		
		Firma	*data*
Approvato da	Direttore Amministrativo		
		Firma	*data*

STORIA DELLE MODIFICHE APPORTATE

Data	Rev.	Motivo del cambiamento
Gennaio 2023	00	Prima emissione

DEFINIZIONI E ABBREVIAZIONI

AOPG: Azienda Ospedaliera di Perugia

Chiavetta USB: o unità flash USB o penna USB (anche in inglese USB flash drive, o pendrive) è una memoria di massa portatile di dimensioni molto contenute che si collega al computer mediante la porta USB.

Dati: l'insieme di informazioni di cui un dipendente o un collaboratore (a prescindere dal rapporto contrattuale con l'Azienda) può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (art. 4 GDPR);

Device (dispositivo): personal computer e altre unità hardware quale periferica/dispositivo elettronico, anche ad alta tecnologia e di piccole dimensioni (smartphone, e-book reader, tablet PC ecc.).

Dipendente: personale dell'ente assunto con qualsiasi tipo di forma contrattuale, anche in stage o tirocinio.

Disciplinare Aziendale: "Disciplinare per il corretto utilizzo degli strumenti informatici, telematici, Internet e Posta Elettronica" (approvato con Delibera del Direttore Generale n. 493/2019), revisionato nell'agosto 2020 (AzOsp_ManOp_13 Rev.1) disponibile sul portale Aziendale

File: porzione di memoria (fissa o mobile) che contiene un insieme organizzato di informazioni omogenee.

GDPR: General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Malware: abbreviazione per malicious software (che significa letteralmente software malintenzionato, ma di solito tradotto come software dannoso), indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata

NIS: Network Information Security – Direttiva Europea che definisce gli standard di sicurezza informatica per gli asset strategici di una nazione, in particolare per gli OSE (Operatori di Servizi Essenziali)

Postazione di lavoro: luogo attrezzato per svolgere un'attività lavorativa dotato di personal computer ed eventuali altre unità hardware.

Rete locale: una Local Area Network (LAN) (in italiano, rete locale) è una rete informatica di collegamento tra più computer, estendibile anche a dispositivi periferici condivisi, che copre un'area limitata, come un'abitazione, una scuola, un'azienda o un complesso di edifici adiacenti.

Virus: programma appartenente alla categoria dei malware che, una volta eseguito, infetta dei file in modo da arrecare danni al sistema, rallentando o rendendo inutilizzabile il dispositivo infetto.

PREMESSA

Il presente documento nasce dall'esigenza dell'Azienda di ridurre al minimo i rischi di sicurezza informatica associati agli accessi dall'esterno del perimetro della rete locale (LAN), oltre a tutelare il patrimonio di dati trattati dall'Azienda.

Con il recepimento della Direttiva Europea NIS (Network Information Security), AOPG ha l'obbligo di innalzare i livelli di sicurezza informatica per garantire la protezione dei dati personali dei propri dipendenti e dei cittadini che usufruiscono dei servizi erogati dall'Azienda. Nel rispetto sia di tale normativa, sia del Regolamento Europeo per la Protezione dei Dati Personali (GDPR).

I dispositivi portatili ed i dati in essi contenuti stanno diventando un obiettivo sempre più comune per i criminali, non solo criminali informatici (cosiddetti hacker) ma vere e proprie organizzazioni volte all'estorsione, allo spionaggio o al terrorismo.

In caso di furto, oltre all'impatto finanziario derivante dalle spese relative alla loro sostituzione, vi sono dei costi tangibili "nascosti" associati, soprattutto, alla reputazione e alla privacy personale associati alla perdita di informazioni sensibili, aziendali o personali anche insostituibili, gestite in tali dispositivi. La perdita rappresentata, sebbene difficile da valutare, rappresenta un elevato costo per AOPG. Siccome ognuno di questi dispositivi potrà contenere informazioni personali, dal punto di vista della sicurezza viene considerato alla stregua di un computer desktop aziendale.

CAMPO DI APPLICAZIONE

Gli standard di sicurezza descritte nel presente documento si applicano a tutti i dipendenti di AOPG che aderiscono al progetto denominato “Smart Working” e che utilizzano un pc portatile di proprietà dell’Azienda oppure usufruiscono del proprio pc portatile personale o device mobile, opportunamente configurato per accedere in sicurezza ai servizi informatici aziendali.

Il disciplinare si applica a tutti i dipendenti, senza distinzione di ruolo o livello, nonché a tutti i collaboratori dell’Azienda Ospedaliera di Perugia a prescindere dal rapporto contrattuale con la stessa intrattenuto (es. collaboratori esterni, Co.co.co., collaboratori a progetto, stagisti, medici in formazione, borsisti ecc.), di seguito “utenti”.

MODALITA’ OPERATIVE

Istruzioni per la custodia degli strumenti per lo Smart Working

Per il corretto utilizzo dei dispositivi aziendali, forniti da AOPG, si rimanda al Disciplinare Aziendale (AzOsp_ManOp_13 Rev.1). L’accesso tramite il dispositivo portatile è consentito al dipendente AOPG nei seguenti casi:

- Internamente all’Azienda, utilizzando la rete di dominio aziendale, cavo o Wi-Fi;
- Dall’esterno di AOPG, dal proprio domicilio utilizzando il collegamento Internet domestico;
- Esternamente ad AOPG in mobilità, utilizzando la rete mobile (cellulare) o Wi-Fi di fornitore noto.

NB: La connessione ad una rete cavo o Wi-Fi pubblica, non conosciuta, quale ad esempio la rete di un hotel o di un locale pubblico, è da evitare in ogni caso, poiché comporta gravi rischi di sicurezza, come il furto delle credenziali dell’utente e l’intercettazione di tutte le informazioni trasmesse e gestite tramite il dispositivo.

I PC portatili e i device mobili sono anche particolarmente vulnerabili alla perdita e al furto. Criminali singoli e organizzati possono commettere il furto sia all'interno degli edifici di AOPG che esternamente all’Azienda. Il rischio è potenzialmente maggiore durante gli spostamenti e quando si viaggia, specialmente se il dipendente AOPG si trova in un ambiente non familiare o si sta concentrando sul viaggio stesso.

Nonostante nella maggior parte dei casi il malvivente tragga profitto dalla vendita del pc portatile sul mercato nero, esiste un numero crescente di criminali che ruba questi dispositivi specificamente per i dati sensibili che possono contenere. Tali informazioni, se rivelate, potrebbero causare danni relativi alla privacy, imbarazzo, perdita di reputazione o significativi effetti finanziari o commerciali per APSS.

Nel contesto lavorativo di AOPG, generalmente le informazioni trattate possono comprendere:

- dati personali sanitari di assistiti e pazienti, informazioni personali relative ai dipendenti;
- qualsiasi informazione personale e privata dell'utente che vorrebbe mantenere privata;
- note di ricerca, dati e informazioni commercialmente sensibili, dati di proprietà intellettuale;
- dati finanziari ed economici.

Per contrastare questi rischi, la sicurezza dei dispositivi mobili viene affrontata in cinque modalità:

a. educazione dell'utente attraverso una maggiore responsabilità e consapevolezza dei rischi e dell'applicazione di una politica di sicurezza dei pc portatili, attraverso la partecipazione ai corsi in “Competenze Digitali in Sanità” organizzati annualmente da AOPG;

b. sicurezza fisica dell'ambiente in cui è custodito o si utilizza il dispositivo portatile, sia all'interno di strutture AOPG, al proprio domicilio che in viaggio;
c. controllo sicuro dell'accesso al dispositivo portatile mediante autenticazione con password sufficientemente robusta (nel rispetto del Disciplinare Aziendale);
d. protezione dei dati conservati sul dispositivo mediante backup e crittografia;
e. tracciamento / cancellazione dei dati, in particolare per i dispositivi ad alto rischio o contenenti dati molto sensibili.

In ogni caso, per limitare danni e perdite di informazioni, si consiglia la minimizzazione della memorizzazione dei dati aziendali sul disco fisso del dispositivo portatile, sia in termini di dimensioni che di tempo.

Al di fuori delle strutture di AOPG, è vivamente sconsigliata la stampa su carta di informazioni aziendali.

Per evitare il furto del dispositivo portatile si consiglia di elevare al massimo il grado di attenzione durante gli spostamenti, sia internamente ma soprattutto al di fuori delle strutture AOPG.

Nel caso in cui si stia lavorando in condizioni di precaria connettività dati dal punto di vista della qualità e continuità del servizio, ad esempio durante un viaggio in treno, è permesso scaricare sul disco locale del dispositivo portatile il documento di lavoro per elaborarlo in modalità offline. A connettività ripristinata, si dovrà copiare il documento nella cartella aziendale, e si dovrà cancellare il documento stesso dal disco locale del dispositivo.

Configurazione dei dispositivi aziendali per lo Smart Working

Le politiche applicate alle postazioni di lavoro aziendali si applicano anche ai dispositivi portatili. Tra queste regole, elencate nel Disciplinare Aziendale, ricordiamo la necessità per tutti gli utenti di accedere alla rete aziendale mediante le credenziali personali, il cambio della password almeno una volta ogni tre mesi o in tutti i casi in cui si ritenga che sia stata inavvertitamente divulgata o compromessa e il logoff automatico dei programmi.

Gli utenti solitamente non dispongono dell'autorizzazione per installare il software o modificare le configurazioni del pc portatile. Tuttavia, la configurazione e l'installazione di particolare software va espressamente richiesta ai Sistemi Informatici tramite il portale Segnalazioni online.

In nessun caso il personale non autorizzato potrà eseguire operazioni di modifica della configurazione dei dispositivi.

Al fine di proteggere le informazioni memorizzate nei portatili, AOPG ha installato un sistema di crittografia del disco che, in caso di tentativi di accesso con password diverse da quella aziendale, rendono illeggibile l'intero contenuto.

Il pc portatile e il device portatile sono abilitati per lavorare in maniera "Smart" tramite la configurazione di tutti i software e i collegamenti necessari.

Utilizzo di dispositivi personali per lo Smart Working

AOPG concede di utilizzare per fini lavorativi il proprio PC portatile o device personale tramite accesso VPN alla rete aziendale. Queste modalità di accesso mettono in sicurezza il transito dei dati sulla rete, ma non sono sufficienti ad eliminare il rischio di violazioni sui dati personali come il furto delle credenziali di autenticazione, la modifica dell'integrità e la diffusione di dati personali. AOPG, infatti, non possedendo il controllo sugli strumenti personali dell'utente, non è in grado di assicurare la sicurezza locale di tali dispositivi, e conseguentemente non può garantire che questo rischio sia ridotto.

È requisito essenziale che i dati abbiano lo stesso livello di sicurezza di quando sono trattati con gli strumenti aziendali messi a disposizione dall'Azienda. Pertanto, l'utente deve provvedere a configurare i propri dispositivi personali con un alto livello di sicurezza, indipendentemente dal tipo di sistema operativo utilizzato, marca e modello del personal computer o del dispositivo mobile.

Al fine di non incorrere in situazioni di vulnerabilità, con conseguenti rischi di violazioni sui dati, l'utente dovrà implementare, a sue spese e sotto la sua responsabilità, le seguenti misure di sicurezza tecniche e comportamentali:

a. verificare costantemente che il proprio personal computer o dispositivo mobile possieda un sistema operativo aggiornato ed applicare costantemente gli aggiornamenti di sicurezza resi disponibili dal produttore;

b. verificare costantemente che sul sistema sia installata una soluzione antivirus e anti-malware di mercato funzionante ed aggiornata, con caratteristiche di protezione in tempo reale dalle minacce, aggiornamenti automatici e scansioni programmate;

c. applicare costantemente gli aggiornamenti di sicurezza di tutte le applicazioni installate sul personal computer o dispositivo personale;

d. verificare costantemente che sul sistema non siano presenti software non conformi o malevoli. In caso contrario, l'utente dovrà provvedere alla loro immediata rimozione.

Si ricorda inoltre che:

- Di norma, i dati aziendali non devono essere memorizzati sul disco locale del personal computer o del dispositivo, né su chiavette USB o dischi esterni di memorizzazione, né su servizi di cloud storage personali;

- se, per motivi di continuità operativa, l'utente dovesse salvare dei dati sui sistemi di memorizzazione non conformi a quanto raccomandato ai punti precedenti, una volta reinseriti e salvati nel sistema gestionale o nell'applicativo aziendale tali dati andranno cancellati dai sistemi di memorizzazione non conformi;

- in caso di contenzioso o indagini dovute a violazioni sui dati aziendali e/o illeciti, l'utente dovrà mettere a disposizione degli inquirenti, per le opportune verifiche sullo stato di sicurezza e sui dati in esso contenuti e per tutto il tempo necessario, il proprio personal computer portatile o dispositivo personale utilizzato per lo Smart Working.

Gestione del rischio

La politica aziendale è quella di consentire al personale di utilizzare i dispositivi portatili come aiuto nello svolgimento del proprio lavoro. I rischi associati a questo utilizzo sono gestiti con le seguenti attività:

- Applicazione di controlli tecnologici come l'accesso con autenticazione forte e il cambio periodico della password;

- controllo antivirus e anti-malware per proteggere i programmi e l'accesso alle informazioni sui dispositivi;

- sul pc portatile di proprietà aziendale, limitazione dei privilegi di accesso in modo che l'utente non possa installare software non aziendale;

- assistenza e formazione agli utenti a comprendere i rischi connessi all'uso di questi dispositivi e come possano essere mitigati al meglio

Rimane responsabilità dell'utente mantenere protetto e custodire il dispositivo, sia aziendale che privato, secondo le politiche di sicurezza contenute in questo documento ed attuare le generali e comuni misure di sicurezza tecniche e comportamentali nell'utilizzo dei dispositivi mobili.

Segnalazione di furto

In caso di furto del dispositivo, sia aziendale che personale, l'utente dovrà denunciare prontamente l'accaduto al Posto Fisso di Polizia o al più vicino commissariato, inviando copia della denuncia ai Sistemi Informatici e Transizione all'Amministrazione Digitale.

RIFERIMENTI NORMATIVI E BIBLIOGRAFIA ESSENZIALE

General Data Protection Regulation - Regolamento Generale sulla Protezione dei Dati - Regolamento (EU) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Network Information Security – Direttiva Europea (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi

Decreto Legislativo 18 maggio 2018, n. 65 - Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

ALLEGATO D

Comunicazione inerente la postazione di lavoro per lo svolgimento del Lavoro agile

La presente comunicazione, dovrà essere compilata e inviata al Responsabile di Struttura, in riferimento al luogo di lavoro prescelto per l'espletamento della prestazione lavorativa in modalità agile, così come individuato nell'accordo individuale.

Nome	Cognome
Matricola	Data di nascita
Codice fiscale	Qualifica
Firma del Lavoratore _____	

Luogo o luoghi di lavoro in modalità agile che si intende adottare per l'espletamento della propria attività (si dovrà indicare un luogo sicuro per la propria salute e sicurezza, esente da situazioni o circostanze pericolose per se stessi e per terzi)	Luogo:_____ _____ Via_____ Città_____ CAP_____
Struttura Complessa di appartenenza	
Attività svolta in modalità agile	_____ _____ _____

SI COMUNICA

Che il luogo di lavoro, inteso come spazio all'interno della sede di lavoro, nel quale si svolge la prestazione lavorativa dovrà rispondere, per quanto possibile, ai seguenti requisiti elencati:

Pareti, pavimenti, soffitti e vie di accesso in corrispondenza della postazione di lavoro

1. Le pareti e i soffitti del luogo di lavoro devono essere in buono stato di conservazione;
2. Il pavimento del luogo di lavoro deve essere regolare e non presentare protuberanze, cavità o asperità;
3. Le vie di accesso ai luoghi di lavoro (corridoi, scale, passaggi) non devono presentare pericoli di inciampo o caduta e/o scivolamento.

Arredi collegati alla postazione di lavoro

4. Gli scaffali/armadi devono essere integri, stabili, privi di pericolo di caduta di oggetti dall'alto sul luogo di lavoro;
5. Non devono essere presenti altri elementi di arredo/oggetti (lampadari, lucernari, quadri, applique etc.) suscettibili di cadere dall'alto.

Postazione di lavoro (allestita o da allestire)

6. Il luogo di lavoro deve garantire sicurezza e riservatezza secondo i criteri e modalità indicati dalla norma e nell'ambito di applicazioni delle linee guida specifiche aziendali;
7. Il lavoratore deve disporre di una apparecchiatura adeguata se di sua proprietà;
8. L'apparecchiatura deve disporre di un proprio cavo originale;
9. L'apparecchiatura, se per il funzionamento deve essere collegata a prolunghe, queste devono essere marcate CE;
10. Il piano di lavoro deve essere, per quanto possibile del tipo antiriflesso;

11. Sul piano di lavoro deve essere presente lo spazio necessario per disporre il monitor, la tastiera e il mouse (sullo stesso piano), nonché per poggiare gli avambracci davanti alla tastiera – Vedi Allegato 1;
12. Nella parte sottostante del piano di lavoro, lo spazio deve essere sufficiente per muovere e distendere le gambe.

Altre informazioni

13. Nel luogo ove viene espletata l'attività lavorativa, deve essere presente un servizio igienico;
14. Nei locali, deve essere possibile mantenere (e regolare) la temperatura dei luoghi di lavoro a livelli non troppo alti o bassi (a seconda della stagione) rispetto alla temperatura esterna.

Disturbi relativi all'apparato visivo

15. L'illuminazione artificiale deve essere adeguata, con tonalità chiara o bianca e avere la possibilità di sistemare dei corpi illuminanti a linea parallela rispetto alle postazioni di lavoro;
16. La posizione degli schermi rispetto alle fonti di illuminazione non deve creare fenomeni fastidiosi di abbagliamento o riflessi (presenza di tendaggi o schermi regolabili e oscuranti);
17. Deve essere possibile adottare lampade in caso di necessità;
18. Lo schermo deve essere posizionato in modo tale, da non riflettere immagini;
19. Lo schermo deve essere perfettamente funzionante ovvero privo di riverberi e sfarfallamenti, e i caratteri devono essere leggibili senza sforzi eccessivi.

Disturbi relativi all'apparato muscolo scheletrico

20. Il tavolo da lavoro deve disporre di una superficie adeguata al tipo di lavoro, in quanto deve essere presente un sufficiente spazio per la tastiera, il mouse e documenti; inoltre l'operatore deve avere la possibilità di adattarli in base alle proprie esigenze (50/70 cm circa);
21. La sedia deve essere stabile e adattabile alle esigenze dell'operatore, con schienale regolabile;
22. La posizione dello schermo deve essere adattabile alle esigenze dell'operatore ;
23. La posizione della tastiera e del mouse, devono essere adattabili alle esigenze dell'operatore (mouse e tastiera muovibili);
24. Lo spazio di lavoro deve avere una superficie sufficiente a garantire i movimenti operativi e i cambiamenti di posizione;
25. In caso di utilizzo di computer portatile e l'operatore è inquadrato come Videoterminalista, solamente in questo caso, è preferibile adottare un mouse e una tastiera ausiliaria.

Collegamento multimediale

26. Il lavoratore deve avere la disponibilità di una rete WI-FI per l'espletamento dell'attività e per il collegamento da remoto;
27. Il lavoratore deve avere la possibilità di collegarsi ad una rete WI-FI per ricevere le comunicazioni o assistenza tecnica in caso di necessità;
28. Il lavoratore deve avere la disponibilità di collegamento ad una rete WI-FI per partecipare a conferenza o momenti di aggregazione con i colleghi.

Consigli per la gestione del lavoro in Smart Working

29. Scegliere un luogo sicuro per la propria salute e sicurezza, esente da situazioni o circostanze pericolose per se stessi e per terzi;
30. Dedicare, se possibile, uno spazio tranquillo della casa ad "ufficio";
31. Programmare la giornata con orari precisi per le pause e per la fine del lavoro;
32. Mantenere una postura eretta durante l'attività lavorativa;
33. Conclusa l'attività spengere il computer e cercare di non continuare a pensare al lavoro;
34. Mantenere i contatti con il responsabile e i colleghi, eventualmente con l'ausilio delle videoconferenze;
35. Pianificare l'attività fisica, sia con esercizi a casa che fuori;
36. Fare le pause;
37. In allegato 1, uno schema di confronto per l'adeguamento della postazione di lavoro.

Allegato 1

VDT: ergonomia del posto di lavoro
La postazione VDT