

Regione Emilia Romagna
Azienda Unita' Sanitaria Locale di IMOLA

DELIBERAZIONE N.134

del 26 SETTEMBRE 2012

Il Direttore Generale, nella sede dell'Azienda Unita' Sanitaria Locale di Imola
– Via Amendola, 2 – nella data sopra indicata, ha assunto la presente deliberazione:

OGGETTO: DISCIPLINARE AZIENDALE IN MERITO ALL'UTILIZZO DI STRUMENTI ELETTRONICI NELL'AMBITO DEL RAPPORTO DI LAVORO (DELIBERAZIONE N. 36 DEL 26.03.2009) MODIFICA.

IL DIRETTORE GENERALE

- richiamata la deliberazione n. 36 del 26 marzo 2009, con la quale è stato approvato il “Disciplinare aziendale in merito all'utilizzo di strumenti elettronici nell'ambito del rapporto di lavoro”;

- dato atto che il Disciplinare detta le regole per l'utilizzo da parte dei lavoratori dei computer e dei servizi di posta elettronica ed internet messi a disposizione dell'Azienda esclusivamente per lo svolgimento dei compiti istituzionali o comunque correlati alla prestazione lavorativa;

- riconosciuta l'esigenza di aggiornare il Disciplinare in argomento, nella parte relativa ai contenuti e ferma restando la disciplina dei controlli (approvata a seguito del procedimento di cui all'art. 4, comma 2, L.300/70);

- dato atto in particolare che il Disciplinare non contempla l'utilizzo dei Social Media e che si ritiene utile prevedere le modalità di attivazione e di utilizzo anche di tali strumenti di comunicazione, sempre più diffusi anche in ambito professionale;

- vista e condivisa la stesura aggiornata del Disciplinare (rispetto al testo approvato con la deliberazione n. 36) integrata con l'art.6 bis (“Social media”) e con modifiche all'art. 7 e all'art. 15 (derivanti da modifiche intervenute sotto il profilo di fatto e sotto il profilo normativo);

- ritenuto quindi di approvare il testo del Disciplinare aggiornato, allegato alla presente deliberazione quale parte integrante e sostanziale;

- viste altresì le istruzioni operative –allegato 2 alla presente deliberazione- che richiamano le condizioni d'uso e le principali norme di riferimento a cui il personale dipendente deve attenersi nell'utilizzo dei social media;

- raccolto il parere favorevole del Direttore Amministrativo e del Direttore Sanitario;

DELIBERA

1) di modificare, come precisato in premessa, il “Disciplinare aziendale in merito all'utilizzo di strumenti elettronici nell'ambito del rapporto di lavoro” approvato con deliberazione n. 36 del 26.3.2009, di cui si allega al presente atto –quale parte integrante e sostanziale- il testo aggiornato;

2) di dare atto che il Disciplinare aziendale allegato sarà diffuso tramite pubblicazione sulla intranet aziendale e sul sito istituzionale dell'azienda unitamente al Codice Disciplinare, nonché tramite invio a tutte le Unità operative complesse aziendali -ivi compresa l'U.O. Risorse Umane- per le finalità di cui all'art. 15 del Disciplinare;

3) di confermare l'informativa ai sensi dell'art. 13 D. Lgs. 196/2003 per dipendenti e terzi non dipendenti, approvata con la deliberazione n. 36 del 26.3.2012, che comunque si allega alla presente deliberazione (allegato n. 2);

4) di approvare le Istruzioni operative social media, contenenti regole di utilizzo e linee guida per i dipendenti, allegato n. 3 alla presente deliberazione;

5) di trasmettere copia del presente provvedimento al Collegio Sindacale, ai sensi della L. R. n.50/94.

F.to IL DIRETTORE GENERALE

Sulla presente delibera hanno espresso parere favorevole

F.to IL DIRETTORE AMMINISTRATIVO

F.to IL DIRETTORE SANITARIO

2012/144

Copia della presente deliberazione, N. 134 del 26/09/2012

viene:

<input checked="" type="checkbox"/>	Publicata all'Albo on line sul sito dell'Ente, in data 28 Settembre 2012 dove rimarrà per quindici giorni consecutivi
<input type="checkbox"/>	Trasmessa alla Regione Emilia Romagna, per il controllo, di cui all'art.4, comma 8 - della Legge 30.12.1991, n. 412, in data
<input type="checkbox"/>	Trasmessa alla Regione Emilia Romagna, per l'autorizzazione di cui all'art.51, comma 1 - della L.R.N. 50/94, in data

F.to L'incaricato

F.to **Il Direttore dell'Unità Operativa
Segreteria Generale e Affari Legali**

Imola, 28 Settembre 2012

La presente deliberazione è divenuta esecutiva in data **28 Settembre 2012**

<input type="checkbox"/>	A seguito della dichiarazione di immediata eseguibilità.
<input checked="" type="checkbox"/>	A seguito della pubblicazione all'Albo on line dell'Ente.
<input type="checkbox"/>	A seguito di <u>controllo favorevole</u> da parte della Regione Emilia Romagna. Autorizzazione con provvedimento N. del

F.to **Il Direttore dell'Unità Operativa
Segreteria Generale e Affari Legali**

Imola, 28 Settembre 2012

La presente deliberazione è stata trasmessa a:

<input checked="" type="checkbox"/>	COLLEGIO SINDACALE	<input checked="" type="checkbox"/>	DIP. AMMINISTRATIVO E TECNICO
<input checked="" type="checkbox"/>	DIREZIONE GENERALE	<input checked="" type="checkbox"/>	U.O. CONTABILITA' E FINANZA
<input checked="" type="checkbox"/>	PROGRAMMAZIONE E CONTROLLO DIREZIONALI	<input checked="" type="checkbox"/>	U.O. SEGRETERIA GEN.LE E AFFARI LEGALI
<input checked="" type="checkbox"/>	INFORMAZIONE E COMUNICAZIONE	<input checked="" type="checkbox"/>	U.O. RISORSE UMANE
<input checked="" type="checkbox"/>	GOVERNO CLINICO	<input checked="" type="checkbox"/>	U.O. INGEGNERIA CLINICA
<input checked="" type="checkbox"/>	FORMAZIONE	<input checked="" type="checkbox"/>	U.O. TECNOL. INFORMATICHE E DI RETE
<input checked="" type="checkbox"/>	RICERCA E INNOVAZIONE	<input checked="" type="checkbox"/>	U.O. PATR. E TECNOL. IMPIANTISTICHE
<input checked="" type="checkbox"/>	DIREZIONE INFERMIERISTICA E TECNICA	<input checked="" type="checkbox"/>	U.O. ECONOMATO E PROVVEDITORATO
<input checked="" type="checkbox"/>	DIREZIONE DELL'ASSISTENZA FARMACEUTICA	<input checked="" type="checkbox"/>	U.O. AMMINISTRAZIONE DEI SERVIZI SANITARI OSPEDALIERI E TERRITORIALI
<input checked="" type="checkbox"/>	DIREZIONE MEDICA DI PRESIDIO	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	DIP. SANITA' PUBBLICA	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	DISTRETTO	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	DIP. CURE PRIMARIE	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	DIP.SALUTE MENTALE E DIPENDENZE PATOLOGICHE	<input type="checkbox"/>	

F.to **Il Direttore dell'Unità Operativa
Segreteria Generale e Affari Legali**

**Disciplinare aziendale in merito all'utilizzo di strumenti elettronici
nell'ambito del rapporto di lavoro**

Sommario

Sezione 1 – Utilizzo strumenti da parte del Lavoratore	2
Art. 1. Condizioni d'uso (computer, posta <i>elettronica</i> e internet)	2
Art.1 bis.....	2
Art. 2. Organizzazione del servizio di posta elettronica: indirizzi di servizio.	2
Art. 3. Organizzazione del servizio di posta elettronica: indirizzi di singoli lavoratori.....	2
Art. 4. Posta elettronica. Indirizzi di singoli lavoratori. Disciplina.....	3
Art. 5. Internet. Abilitazioni e utilizzo.	3
Art. 6. Computer	4
Art. 6-bis Social Media	4
Sezione 2 – Trattamento dati. Disciplina aziendale	4
Art. 7. Trattamento dei dati. Scopo.	4
Art. 8. Trattamento dati. Soggetti preposti.....	4
Art. 9. Controlli. Modalità.....	5
Art. 10. Conservazione dei dati.....	6
Art. 11. Comunicazione e diffusione	6
Art. 12. Informativa art.13 D.lgs. 196/2003.....	6
Art. 13. Accesso ai dati	6
Art. 14. Utilizzo indebito degli strumenti elettronici. Responsabilità.....	6
Art.15. Pubblicizzazione.	6

Sezione 1 – Utilizzo strumenti da parte del Lavoratore

Art. 1. Condizioni d'uso (computer, posta elettronica e internet)

1. L'Azienda mette a disposizione dei lavoratori computer, servizi di posta elettronica e internet, esclusivamente per lo svolgimento di compiti istituzionali o comunque correlati alla prestazione lavorativa.
2. Non è consentito ai lavoratori utilizzare per motivi e fini personali/privati gli strumenti di che sopra, di cui i lavoratori dispongono per ragioni di ufficio.
3. Il divieto opera anche al di fuori dell'orario di lavoro ed è da intendersi assoluto cioè riferito anche a utilizzi (per ragioni personali) occasionali e limitati.
4. E' automaticamente inserita nei messaggi di posta elettronica la seguente avvertenza, anche a tutela della riservatezza di terzi: *"Si informa che la presente casella di posta è destinata esclusivamente a comunicazioni di tipo istituzionale e che eventuali messaggi di risposta potranno essere conosciuti nell'ambito dell'organizzazione dell'Azienda USL di Imola. Le informazioni contenute in questa comunicazione sono riservate e destinate esclusivamente alla/e persona/e (in qualità di dipendente) o all'ente sopra indicati. E' vietato ai soggetti diversi dai destinatari qualsiasi copia-diffusione di quanto in esso contenuto sia ai sensi dell'art. 616 c.p. sia ai sensi del DL n.196/03. Se questa comunicazione Vi è pervenuta per errore, Vi preghiamo di rispondere a questa e-mail e successivamente cancellarla dal Vostro sistema"*
5. I lavoratori che hanno in carico indirizzi di p.e. sono tenuti a mantenere nei messaggi di posta elettronica l'avvertenza di che sopra e rispondono di eventuali contestazioni da parte di terzi derivanti dalla mancata avvertenza.

Art.1 bis.

1. Per qualsiasi strumentazione informatica utilizzata dalle Organizzazioni Sindacali, dalle rappresentanze delle RSU e dai RLS si fa rinvio a separati accordi.

Art. 2. Organizzazione del servizio di posta elettronica: indirizzi di servizio.

1. Di norma ciascun servizio/Unità Operativa è dotato di una casella di posta elettronica, condivisa da più lavoratori.
2. In relazione alla eventuale articolazione del servizio/unità operativa in più settori/uffici, con distinti ambiti di competenza, la casella di servizio potrà essere affiancata da ulteriori caselle per i suddetti uffici/settori, individuati dal Responsabile del servizio/unità operativa, condivisi da più lavoratori.
3. Spetta al Responsabile del servizio/unità operativa definire le regole di gestione finalizzate ad assicurare la presa in carico delle comunicazioni elettroniche e la gestione delle stesse garantendo la continuità; potrà ad esempio essere incaricato un operatore (con sostituto) per la lettura e l'assegnazione dei messaggi di posta elettronica.
4. Resta fermo quanto previsto nel Manuale di gestione dei documenti amministrativi, *pubblicato sulla intranet aziendale.*

Art. 3. Organizzazione del servizio di posta elettronica: indirizzi di singoli lavoratori.

1. La eventuale attribuzione di indirizzi di posta elettronica a singoli dipendenti deve essere autorizzata dal Responsabile del servizio/unità operativa.
2. Il Responsabile, a tale fine, valuta (e si attiene) ai seguenti criteri:
 - numerosità delle comunicazioni (derivante dalle specifiche mansioni del dipendente) tale da rendere più funzionale una gestione separata rispetto alla casella di servizio;
 - e/o esigenze di riservatezza (derivanti da specifiche mansioni/ruoli).

Disciplinare aziendale in merito all'utilizzo di strumenti elettronici nell'ambito del rapporto di lavoro

Art. 4. Posta elettronica. Indirizzi di singoli lavoratori. Disciplina.

1. Il lavoratore titolare di indirizzo di posta elettronica assicura la presa in carico delle comunicazioni elettroniche e la gestione delle stesse, garantendo la continuità.
2. L'azienda mette a disposizione dei lavoratori titolari di indirizzo di posta elettronica apposita funzionalità per l'invio automatico, in caso di assenza programmata, di messaggio di risposta contenente le coordinate per contattare altro settore aziendale (che interviene in sostituzione del lavoratore assente).
3. Il lavoratore titolare di indirizzo di p.e. ha l'obbligo di attivare tale funzionalità in occasione di assenze programmate e risponde di eventuali conseguenze pregiudizievoli – disfunzioni che possano derivare dalla mancata attivazione. *Si allega apposita istruzione per l'attivazione della funzionalità.*
4. In caso di assenza non programmata, superiore a 3-10 giorni (la variabile è valutata in relazione alle mansioni del dipendente) il Responsabile del servizio può disporre l'attivazione della suddetta funzionalità, tramite personale appositamente incaricato (possibilmente coincidente con il lavoratore di cui al comma successivo), dandone poi informazione al personale interessato.
5. Il dipendente titolare di indirizzo di p.e. è tenuto inoltre a delegare, utilizzando l'apposita modulistica, ad altro lavoratore del servizio/unità operativa di appartenenza o al Responsabile del Servizio di appartenenza, l'accesso alla casella di posta e la lettura dei messaggi.
6. Quanto sopra per poter far fronte, in caso di assenze non programmate e protratte nel tempo a improrogabili esigenze di servizio che rendano necessario l'accesso al contenuto dei messaggi di posta elettronica.
7. Il lavoratore delegato assume la gestione dei messaggi di posta elettronica secondo le regole definite dal responsabile dell'Unità Operativa. Di tali operazioni sarà data informazione al delegante
8. Il lavoratore ha a disposizione una casella di posta della dimensione di 80 Mb, ed è tenuto a scaricare localmente i messaggi di posta periodicamente al fine di evitare il riempimento della casella di posta.
9. Le caselle di posta non movimentate per più di tre mesi saranno disattivate d'ufficio.
10. Prima dell'attivazione dell'indirizzo di p.e. il lavoratore sottoscrive apposite istruzioni operative, visionabili anche sulla intranet aziendale.

Art. 5. Internet. Abilitazioni e utilizzo.

1. La navigazione internet è libera e consentita a tutti gli utenti di rete, senza specifica abilitazione, sui siti elencati nella intranet aziendale, individuati in relazione alla connessione dei siti stessi con l'attività istituzionale dell'Azienda e su tutti i siti di inquadriati nelle categorie Education, Health e Government del software di web filtering Websense in modo da consentire il libero utilizzo delle risorse bibliografiche elencate nelle pagine intranet della Biblioteca aziendale.
Compete ai responsabili di servizio segnalare al Responsabile TIR nuovi siti da inserire nella lista; è facoltà del TIR acquisire la conferma della richiesta dal Responsabile del Dipartimento o della Direzione Tecnica di riferimento.
2. L'abilitazione dei singoli lavoratori all'accesso ad Internet è autorizzata dal Responsabile del servizio/unità operativa, valutando discrezionalmente l'utilità dello strumento rispetto alle mansioni di singoli lavoratori e tenendo conto dei contenuti della lista di cui al comma 1, e può, eventualmente, essere configurata secondo i seguenti parametri:
 - ambiti di navigazione;
 - tempo assegnato (su base periodica);
 - volume di byte trasferiti (su base periodica) .
3. Contestualmente all'abilitazione il lavoratore sottoscrive apposite istruzioni operative, visionabili anche sulla intranet aziendale.
4. L'azienda utilizza sistemi che prevengono l'accesso a siti ritenuti non pertinenti (black list), e altre operazioni (quali download di file o software con particolari caratteristiche dimensionali o di tipologia di dato). Tali sistemi sono gestiti dall'UOTIR. e generano un messaggio automatico che avvisa il dipendente dell'avvenuta rilevazione di un uso non autorizzato della rete. Qualora il lavoratore rilevi, incidentalmente, l'accessibilità a siti con contenuti inopportuni, lo segnala all'UOTIR.

Disciplinare aziendale in merito all'utilizzo di strumenti elettronici nell'ambito del rapporto di lavoro

5. Il personale è autorizzato al download di file per uso esclusivo professionale, non sono consentiti download di file musicali. Non è consentito download software a meno di aggiornamenti per abbonamento. Non è altresì consentito l'utilizzo di software di download peer to peer.

Art. 6. Computer

1. Relativamente al computer in dotazione di singoli dipendenti, si applicano i principi di cui all'Art. 4, e precisamente il dipendente è tenuto a delegare ad altro lavoratore o al Responsabile del Servizio di appartenenza, l'accesso al proprio computer, sulla base di apposite istruzioni tecniche.
2. Quanto sopra per poter far fronte, in caso di assenza, ad improrogabili esigenze di servizio che rendano necessario l'accesso al computer.
3. E' opportuna l'indicazione *nei documenti (a fondo pagina)* della denominazione del file (per consentire un accesso mirato).

Art. 6-bis. Social Media

1. In fase di richiesta dell'abilitazione all'utilizzo di internet tramite gli appositi moduli reperibili sulla intranet aziendale, i Responsabili di Unità Operativa specificano se il lavoratore deve essere autorizzato all'utilizzo dei social media.
2. La scelta in merito ai lavoratori da abilitare è effettuata dal responsabile di unità operativa tenendo conto del ruolo e delle mansioni degli operatori stessi, nonché dell'utilità dell'abilitazione ai fini professionali/istituzionali.
3. Prima dell'abilitazione per l'utilizzo dei social media, il lavoratore sottoscrive apposite istruzioni operative, visionabili anche sulla intranet aziendale.

Sezione 2 – Trattamento dati. Disciplina aziendale

Art. 7. Trattamento dei dati. Scopo.

1. L'azienda tratta dati connessi all'utilizzo degli strumenti elettronici, anche riferibili ai lavoratori, per lo svolgimento di proprie funzioni istituzionali e precisamente per garantire la sicurezza e la funzionalità del sistema nonché la continuità dei servizi.
2. In questi casi, qualora i sistemi possano determinare in via incidentale ed indiretta un controllo a distanza sull'uso degli strumenti elettronici da parte dei lavoratori, devono essere rispettate le procedure e le garanzie di cui all'art. 4 L.300/70, il provvedimento del Garante per la protezione dei dati personali del 1.3.2007, nonché le disposizioni di cui al D.Lgs.196/2003 ed il presente atto.
3. E' comunque escluso il trattamento di dati personali mediante sistemi hardware e software finalizzati al controllo a distanza dei lavoratori, svolti, in particolare, mediante:
 - la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
 - la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
 - la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
 - l'analisi occulta di computer affidati in uso;
4. Può essere effettuato l'accesso da remoto da parte del personale TIR alle postazioni PC in caso di malfunzione della postazione. Il lavoratore che utilizza la postazione è avvertito dell'accesso remoto mediante un cambiamento di colore della corrispondente icona sulla barra di controllo delle applicazioni. Tale informazione è ben evidenziata nella informativa di cui al successivo art. 12.

Art. 8. Trattamento dati. Soggetti preposti.

1. Il Responsabile del trattamento è il Responsabile dell'UOTIR, che si attiene alle disposizioni di cui al presente atto, specie per ciò che concerne il divieto di cui all'art. 7 comma 3, la conservazione dei dati e le modalità dei controlli.

Disciplinare aziendale in merito all'utilizzo di strumenti elettronici nell'ambito del rapporto di lavoro

2. In analogia ad altri trattamenti sono incaricati del trattamento tutti gli operatori del servizio TIR (vincolati dal segreto d'ufficio). Sono predisposte dal responsabile dell'UOTIR specifiche istruzioni operative inerenti tali trattamenti, anche e soprattutto al fine di garantire quanto prescritto all'art. 7 ed ai successivi artt. 9 e 10.
3. L'accesso a tali dati è consentito al personale del TIR al fine della verifica delle anomalie tecniche e di traffico usando accortezze che consentano nella maggior parte dei casi l'oscuramento dei dati identificativi individuali.
4. Nel caso in cui siano affidate a terzi prestazioni, quali interventi di manutenzione, gli atti contrattuali devono prevedere la nomina dell'organismo terzo quale responsabile esterno del trattamento ed il vincolo al rispetto delle istruzioni operative impartite dall'azienda.

Art. 9. Controlli. Modalità

1. Fatto salvo quanto precisato all'art. 7, il controllo indiretto sull'uso degli strumenti elettronici da parte dei lavoratori si attiene ai principi di necessità pertinenza e non eccedenza rispetto alle finalità di sicurezza, prevenzione di incidenti e danni, nonché ai principi di trasparenza ed imparzialità; sono quindi escluse interferenze ingiustificate e controlli prolungati, costanti o indiscriminati.
- 2.. Il TIR esegue periodiche verifiche di sicurezza, aventi ad oggetto dati generali, consistenti in:
 - verifiche giornaliere sui log del sistema firewall
 - verifiche dei software installati sui sistemi server e client
 - verifiche sul traffico di rete
 - verifiche sull'efficienza dei sistemi proxy
 - verifiche sui sistemi antivirus
 - verifiche sull'efficacia dei filtri antispam (ex comma 3)
3. Se dalle verifiche sul traffico di rete e sui log di sistema emergono siti palesemente a valenza non istituzionale, il TIR li inserisce nella black list.
4. I controlli potranno essere di due diverse tipologie:
 - **controlli puntuali** (individuali), si attivano:
 - a. **a seguito di malfunzione;** l'ufficio competente alla manutenzione dei sistemi (UOTIR) provvede a identificare UTENTE / PASSWORD che hanno determinato il danno alla postazione e segnala al responsabile della UO il dipendente corrispondente alla identità elettronica identificata
 - b. **a seguito di eventi di danno o di pericolo di danno emersi nell'ambito delle verifiche di sicurezza** (incidenti di sicurezza su postazioni specifiche)

i controlli si riferiscono ai dati relativi ad un periodo non superiore ai 20 giorni anche consecutivi.

- **controlli a campione:**

Periodicamente e comunque a intervalli non inferiori ad 1 mese, l'UOTIR può effettuare controlli a campione in giornate identificate mediante un generatore di numeri casuali. In tal modo seleziona una giornata nell'arco del mese precedente l'estrazione; il controllo è effettuato sui log di navigazione internet della giornata estratta e dei 3 giorni successivi alla stessa.

Il campione è costituito da una percentuale pari allo 0,2% degli indirizzi IP individuati mediante un generatore di numeri casuali.

Le estrazioni sono pubbliche e la giornata dell'estrazione è comunicata mediante la Intranet aziendale.

Nel caso in cui si riscontri un possibile utilizzo improprio delle strumentazione informatiche, il Responsabile del TIR associa il nominativo dell'utilizzatore all'indirizzo IP.

5. In tutti casi di controllo di cui al punto 4, qualora sia ipotizzato un utilizzo improprio delle strumentazioni informatiche, il Responsabile del TIR dà informazione al lavoratore interessato, con possibilità di contraddittorio e, qualora necessario ai fini istruttori, al relativo Responsabile. Il Responsabile, sentito il lavoratore, valuterà l'attinenza dei dati rispetto all'attività lavorativa. A seguito dell'avvenuto accertamento dell'utilizzo improprio delle attrezzature informatiche, il responsabile attiva le procedure disciplinari di cui all'art. 14.,finalizzate, al primo comportamento accertato, all'applicazione del richiamo, salvo casi di particolare gravità. Delle sanzioni applicate viene data informazione anche al Direttore generale.

Disciplinare aziendale in merito all'utilizzo di strumenti elettronici nell'ambito del rapporto di lavoro

Art. 10. Conservazione dei dati.

1. Sono conservati i dati inerenti il traffico internet (log di navigazione) per un periodo non superiore ad 1 mese, tali dati non sono oggetto di archiviazione di backup.
2. Sono conservati i messaggi di posta elettronica per un periodo non superiore a 1 mese (salvo riempimento delle caselle di posta, in tal caso si veda quanto previsto all'art. 4), tali archivi sono oggetto di backup giornaliero ma non hanno archivio storico collegato.
3. Il periodo di conservazione di cui ai commi precedenti può essere superato in caso di richiesta dell'autorità giudiziaria o di polizia giudiziaria per indagini in corso, nonché, in via eccezionale, a fronte di fatti illeciti già accaduti.

Art. 11. Comunicazione e diffusione

1. I dati inerenti il traffico Internet e la posta elettronica non sono in alcun modo oggetto di diffusione. Sono eventualmente oggetto di comunicazione su richiesta dell'autorità giudiziaria e/o qualora necessari a difesa dell'azienda in ambito giudiziale.

Art. 12. Informativa art.13 D.lgs. 196/2003

1. L'informativa fornita al dipendente ai sensi dell'art.13 D.lgs. 196/2003 in ordine al complesso dei trattamenti dati collegati alla gestione del rapporto di lavoro contiene anche le opportune informazioni inerenti il trattamento dei dati riguardanti la navigazione internet e la posta elettronica. L'informativa è pubblicata sulla intranet aziendale (previo avviso a tutti i dipendenti) e consegnata al momento dell'assunzione.

Art. 13. Accesso ai dati

1. L'accesso ai dati analitici (contenenti riferimenti individuali) è consentito ai lavoratori interessati su richiesta e con la mediazione tecnica di un operatore autorizzato della UOTIR. L'istanza di accesso è autorizzata dal Responsabile del trattamento.

Art. 14. Utilizzo indebito degli strumenti elettronici. Responsabilità

1. I lavoratori rispondono ai sensi di legge in sede civile, penale ed amministrativa (per danno erariale) per l'illecito utilizzo degli strumenti elettronici messi disposizione dall'Azienda.
2. Inoltre ferme restando le disposizioni di legge per le citate responsabilità (civile, penale ed amministrativa) l'utilizzo improprio degli strumenti elettronici può essere oggetto delle sanzioni disciplinari previste dal CCCCNNLL, secondo le procedure ivi definite. Per il personale dirigente, fatta salva la responsabilità disciplinare per i casi di estrema gravità, l'accertato utilizzo improprio rientrerà nella procedura di valutazione degli incarichi dirigenziali.
3. Per le sanzioni, le procedure e le competenze, si fa rinvio al codice disciplinare affisso nei luoghi di lavoro.

Art.15. Pubblicizzazione.

1. Il presente Disciplinare viene pubblicizzato con le stesse modalità in uso per il Codice Disciplinare.
2. È depositato presso tutte le Unità Operative Complesse aziendali a disposizione del personale per la consultazione.
3. Il Disciplinare è consegnato in copia al personale all'atto dell'assunzione.

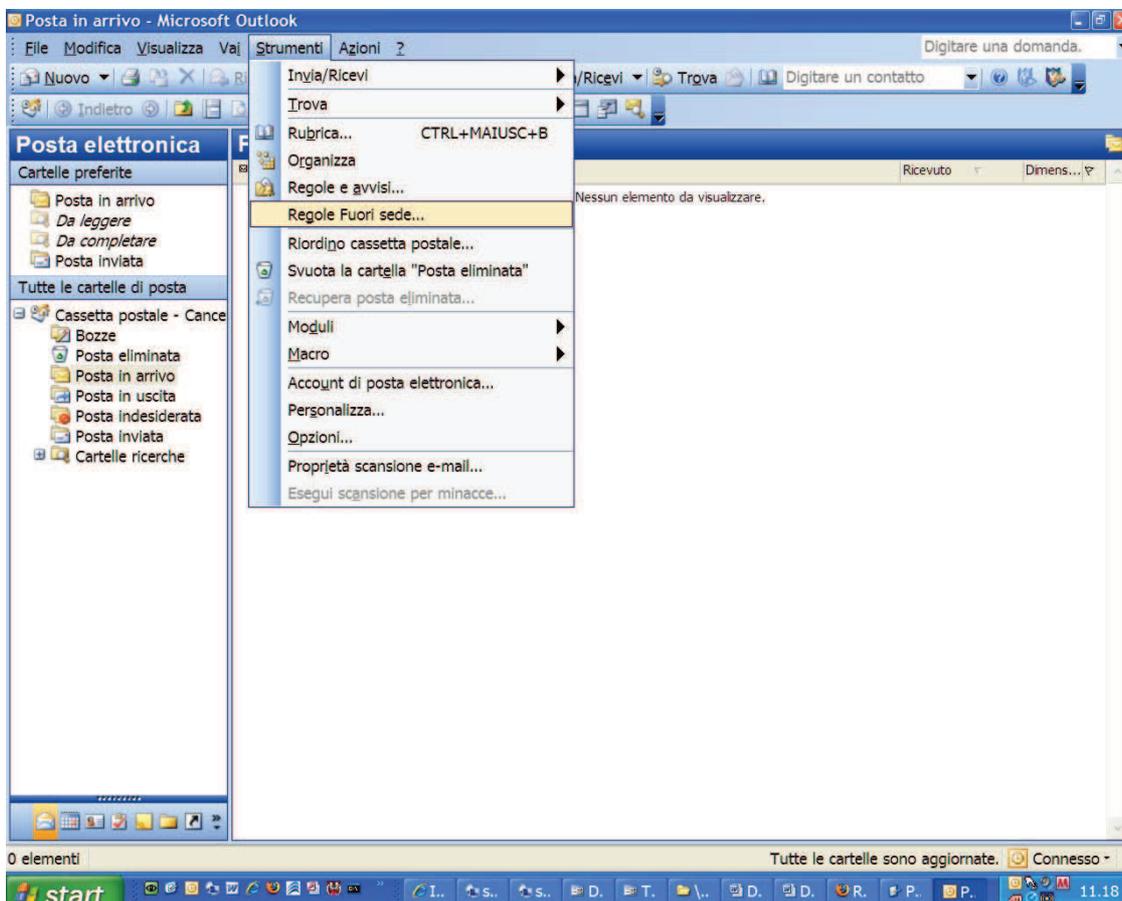
Dipartimento Amministrativo-Tecnico
U.O. Tecnologie Informatiche e di Rete

ISTRUZIONI OPERATIVE PER L'ATTIVAZIONE "FUORI SEDE"

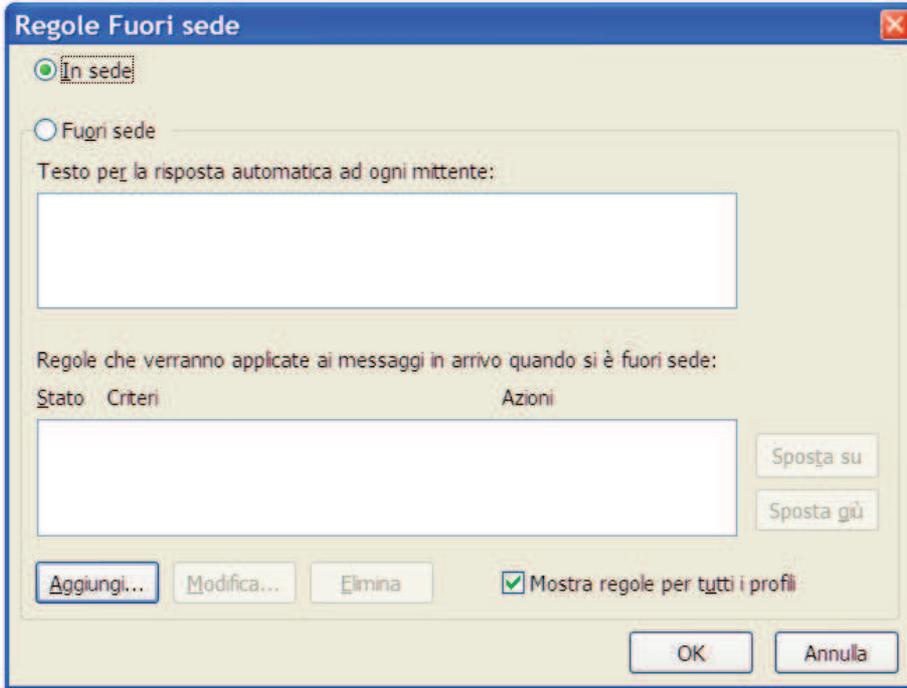
Il Disciplinare aziendale in merito all'utilizzo di strumenti elettronici nell'ambito del rapporto di lavoro obbliga il titolare di indirizzo di posta elettronica ad attivare l'apposita funzionalità per l'invio automatico, in caso di assenza programmata, di un messaggio di risposta contenente le coordinate per contattare altro settore aziendale (che interviene in sostituzione del lavoratore assente).

Istruzioni Operative Per Outlook 2003 e per Outlook 2000

Dal menù **Strumenti** selezionare la voce **Regole Fuori sede...**

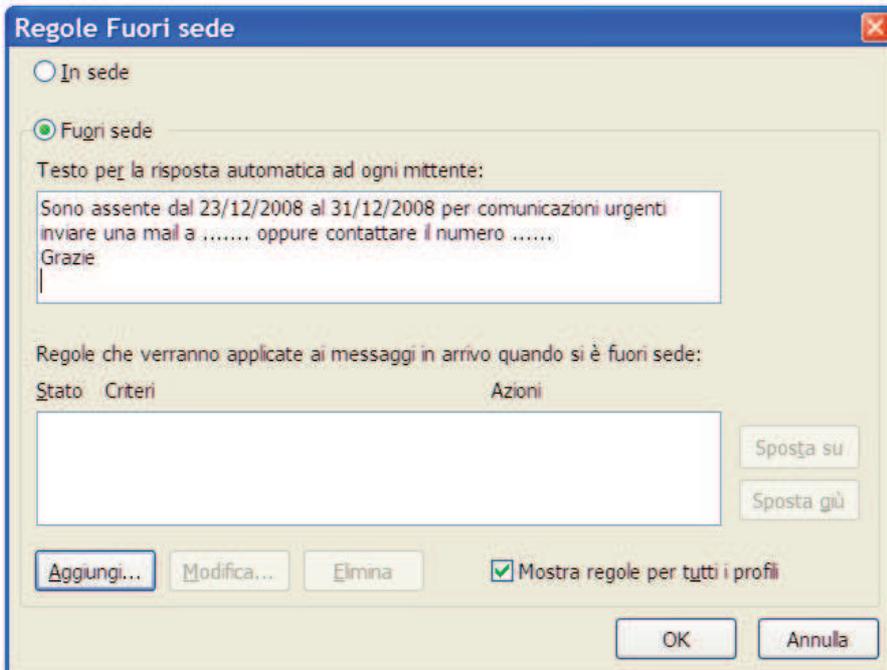


Selezionando **In sede** l'invio della risposta automatica al mittente sarà disattivato:



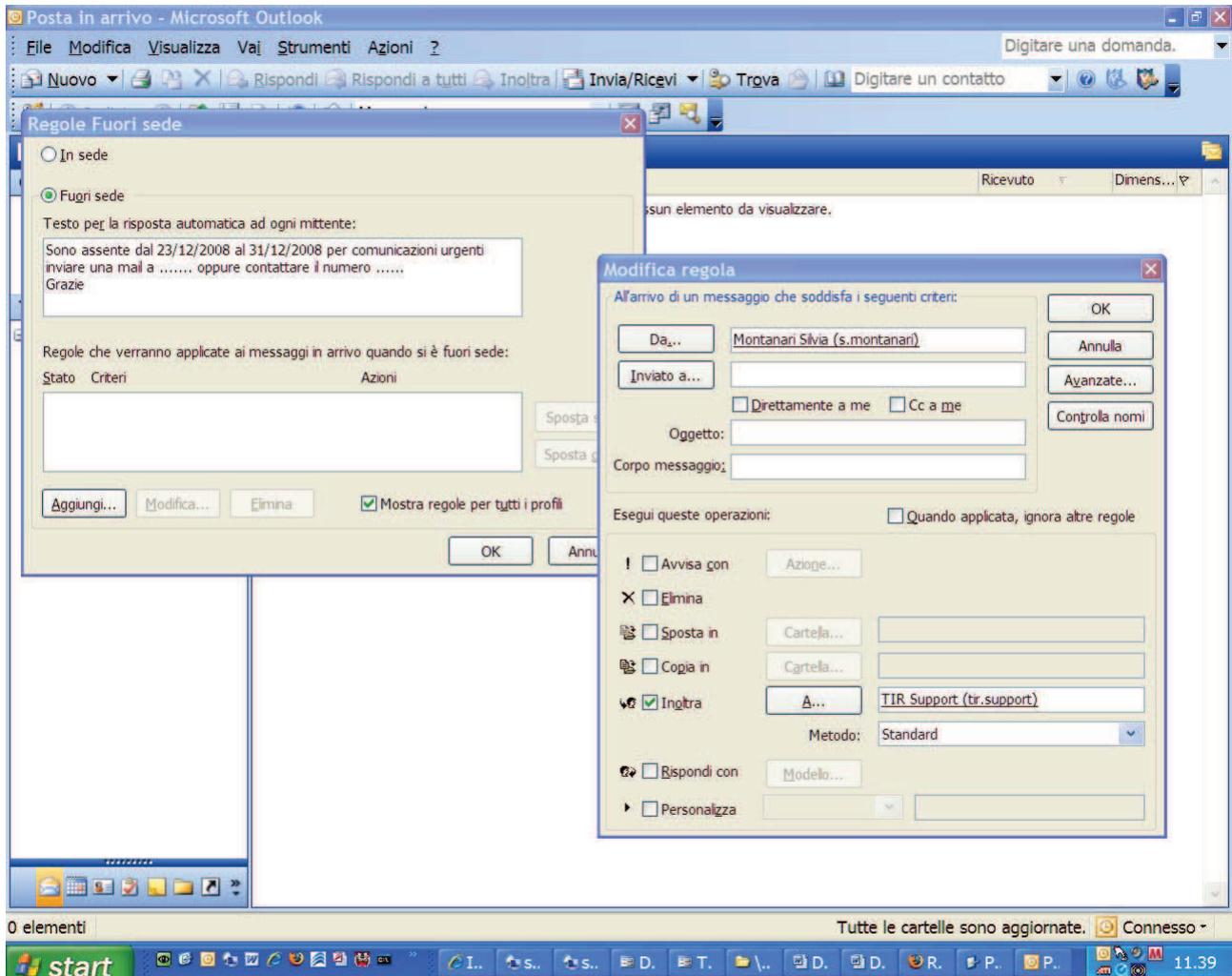
The screenshot shows a dialog box titled "Regole Fuori sede". At the top, there are two radio buttons: "In sede" (selected) and "Fuori sede". Below the "In sede" option, there is a text area labeled "Testo per la risposta automatica ad ogni mittente:" which is currently empty. Underneath, there is a section for rules with a table header: "Stato", "Criteri", and "Azioni". The table body is empty. To the right of the table are two buttons: "Sposta su" and "Sposta giù". At the bottom of the dialog, there are three buttons: "Aggiungi...", "Modifica...", and "Elimina". A checkbox labeled "Mostra regole per tutti i profili" is checked. At the very bottom are "OK" and "Annulla" buttons.

Selezionando invece l'opzione **Fuori sede** verrà inviato in automatico un messaggio ad ogni mittente con il testo specificato sotto.



The screenshot shows the same "Regole Fuori sede" dialog box, but now the "Fuori sede" radio button is selected. The text area for the automatic response now contains the following text: "Sono assente dal 23/12/2008 al 31/12/2008 per comunicazioni urgenti inviare una mail a oppure contattare il numero Grazie". The rest of the dialog box, including the table and buttons, remains the same as in the previous screenshot.

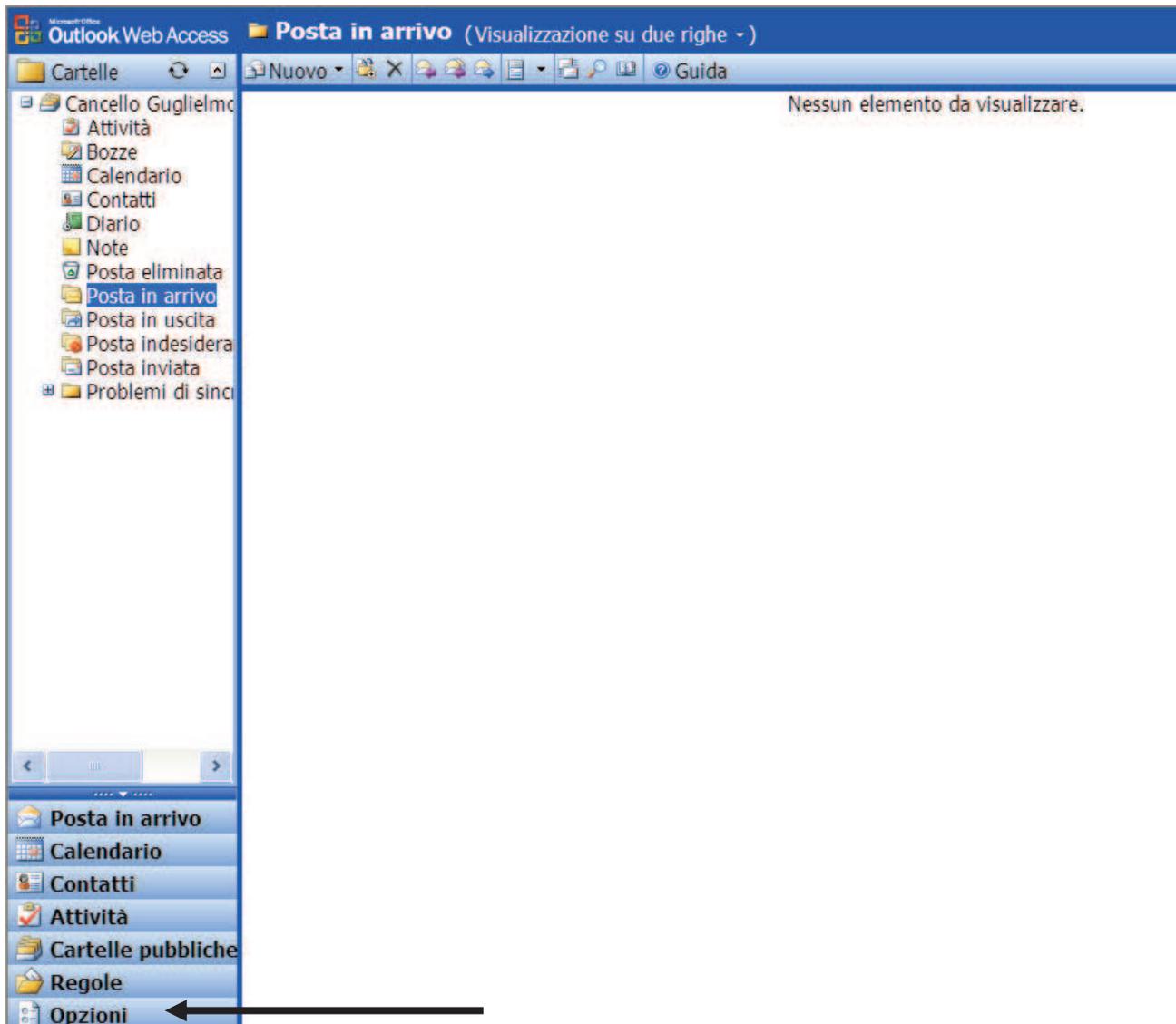
E' possibile inoltre stabilire ulteriori regole premendo il pulsante **Aggiungi**. Nell'esempio che segue tutte le mail provenienti da s.montanari@ausl.imola.bo.it verranno inoltrate all'indirizzo tir.support@ausl.imola.bo.it.



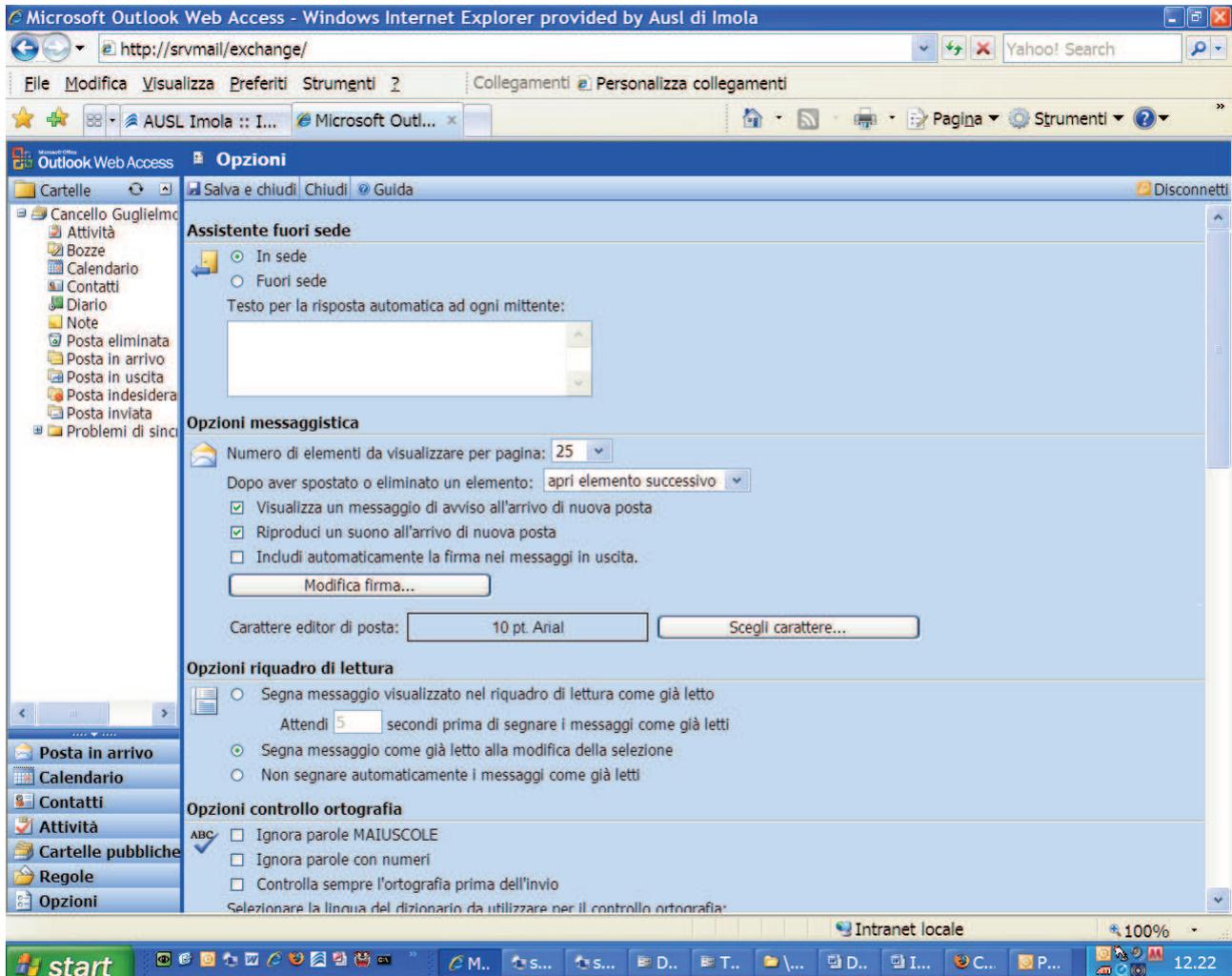
Istruzioni Operative per Outlook Web Access

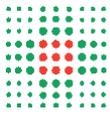
(accesso alla posta elettronica tramite browser)

Dopo essersi collegati alla cassetta di posta tramite internet, dal menù a sinistra selezionare **Opzioni**



Selezionando **In sede** l'invio della risposta automatica al mittente sarà disattivato mentre selezionando **Fuori sede** è possibile impostare il messaggio da inviare in automatico a tutti i mittenti.





Allegato B al Disciplinare Aziendale

All'U.O. T.I.R.

e, p.c. Al responsabile del servizio (1*) _____

Ai sigg.(2*) _____

Oggetto: casella di posta elettronica (p.e.) e personal computer (p.c.) - Delega.

Io sottoscritto _____, matricola n. _____, in servizio presso _____, indirizzo di p.e. _____, in relazione a quanto previsto dal "Disciplinare per l'utilizzo degli strumenti elettronici nell'ambito del rapporto di lavoro"

DELEGO

a _____, indirizzo p.e. _____ e, in subordine, in caso di contemporanea assenza a _____ indirizzo di p.e. _____, da me già informati

- la gestione della casella di p. e. indirizzo _____, in caso di mia assenza non programmata;
- l'accesso al p.c. in dotazione, n. inventario _____, in caso di mia assenza;
- l'attivazione della funzionalità di risposta automatica in caso di mia assenza non programmata

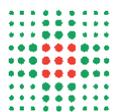
Quanto sopra, per i primi due punti, se necessario per esigenze di servizio non prorogabili, come tali valutate dal Responsabile del servizio.

Data _____

Firma _____

(1*) Indicare il Servizio di appartenenza.

(2*) Indicare i Delegati.



**INFORMATIVA AI SENSI DELL'ART.13 DEL "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" (CODICE PRIVACY) DEL
30.6.2003 N.196**

**COMUNICATO PER DIPENDENTI E TERZI NON DIPENDENTI (LIBERI PROFESSIONISTI, CONSULENTI, DOCENTI,
CONVENZIONATI, ETC)**

Gentile Signora / Signore

La informiamo che ai sensi del "Codice in materia di protezione dei dati personali" il trattamento delle informazioni che La riguardano da parte dell'Azienda U.S.L. di Imola si svolgerà nel rispetto dei diritti e libertà fondamentali, con particolare riferimento alla riservatezza delle informazioni e alla protezione dei dati personali.

Il trattamento dei dati personali sarà, quindi, improntato a principi di correttezza, liceità, legittimità, indispensabilità e non eccedenza rispetto agli scopi per i quali i dati stessi sono raccolti.

LE FINALITA' PER LE QUALI L'AZIENDA U.S.L. TRATTA I SUOI DATI

Le informazioni personali, sensibili e giudiziarie che La riguardano vengono trattate esclusivamente per le seguenti finalità:

- a) **amministrative**, connesse cioè alla instaurazione, gestione e risoluzione dei rapporti di lavoro di qualunque tipo dipendente o autonomo, a tempo parziale o temporaneo e di altre forme di contratto che non comportano la costituzione di un rapporto di lavoro subordinato. A titolo esemplificativo si riportano i trattamenti effettuati al fine di:
- accertare il possesso di particolari requisiti previsti per l'accesso all'impiego o per l'idoneità/inidoneità allo svolgimento delle mansioni/servizio ovvero per il riconoscimento della dipendenza da causa di servizio di infermità o malattie professionali;
 - adempiere ad obblighi in materia di igiene e sicurezza del lavoro nonché in materia sindacale
 - svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile
 - applicare la normativa in materia di incompatibilità
 - gestire l'organizzazione di attività formative;
- b) **contabili**, connesse cioè all'assolvimento di obblighi retributivi, fiscali e previdenziali.

La informiamo che potranno essere trattati dati personali e/o sensibili riguardanti i Suoi familiari solo se espressamente forniti in quanto indispensabili per l'erogazione di benefici o agevolazioni.

Il trattamento dei dati è indispensabile per poter gestire il rapporto di lavoro o l'attività svolta a favore dell'Azienda, sotto il profilo economico e giuridico, in assolvimento di norme di legge o di regolamento, o comunque in stretta correlazione con le competenze istituzionali in materia.

Il conferimento dei dati richiesti alla S.V. riveste natura obbligatoria.

I Suoi dati (personali, sensibili o giudiziari) sono trattati da incaricati individuati sia tra il personale dell'Azienda che appartiene alle Unità Operative a cui a fanno capo o che concorrono ai trattamenti ovvero da soggetti terzi che forniscono servizi elaborativi su richiesta dell'Azienda.

L'Azienda inoltre tratta dati connessi all'utilizzo degli strumenti elettronici (internet, posta elettronica, p.c.) da parte dei lavoratori e può disporre controlli. Sulle condizioni di utilizzo degli strumenti elettronici, sul trattamento dei dati e sui controlli, si fa rinvio al "**Disciplinare aziendale in merito all'utilizzo di strumenti elettronici nell'ambito del rapporto di lavoro**" pubblicato sulla intranet aziendale ed affisso nei luoghi di lavoro unitamente al Codice Disciplinare.

Potrà trovare l'elenco delle disposizioni normative ed un dettaglio sulle finalità e caratteristiche dei trattamenti collegati alla gestione dei rapporti di lavoro nel Regolamento Regionale n.3 del 24 aprile 2006, Allegato B, in particolare schede 43,44,33,36.

LA SICUREZZA DEI DATI

L'Azienda U.S.L. custodisce i dati sia in archivi cartacei sia informatici, nel rispetto dei principi e delle regole concernenti le misure minime di sicurezza per evitare rischi di perdita, distruzione o accesso non autorizzato. L'Azienda adotta annualmente, entro il 31 marzo, il Documento Programmatico sulla sicurezza, riportante anche l'individuazione degli amministratori di sistema. Tale documento è pubblicato sulla intranet aziendale Normative e Regolamenti - Privacy - Documento programmatico della sicurezza

LA COMUNICAZIONE DEI DATI

I dati raccolti potranno essere comunicati nei limiti e nei casi consentiti dalla normativa (cfr. Regolamento regionale n.3) e per le sole finalità sopra esposte, ad enti pubblici o privati, quali, ad esempio:

- a) ad altre Aziende Sanitarie ed Ospedaliere;
- b) ad enti previdenziali (es. INPDAP e INPS);
- c) ad altri soggetti pubblici (esempio Regione e Comuni, Amministrazione finanziaria, Commissioni e Comitati di verifica per le cause di servizio, INAIL etc.) o privati, a cui siano affidati compiti per finalità istituzionali da parte dell'Azienda U.S.L. di Imola (es. Tesoriere, Studi Legali)
- d) all'Autorità Giudiziaria e/o all'Autorità di Pubblica Sicurezza, nei casi espressamente previsti dalla legge.

Inoltre potranno venire a conoscenza dei Suoi dati i Responsabili di trattamento (anche esterni) nominati dall'Azienda, gli incaricati dei trattamenti afferenti ad articolazioni organizzative dell'Azienda, entrambi individuati con apposite deliberazioni annuali (vd. punto successivo) e gli amministratori di sistema (individuati nel richiamato Documento programmatico per la Sicurezza).

TITOLARI E RESPONSABILI PRESSO L'AZIENDA U.S.L. DI IMOLA

Titolare del trattamento è l'Azienda U.S.L. di Imola – viale Amendola 2, 40026 Imola

L'elenco dei trattamenti e dei relativi Responsabili può essere visionato presso l'Ufficio Relazioni con il Pubblico (Viale Amendola 2), presso le portinerie dei presidi dell'Azienda U.S.L. di Imola ed è altresì pubblicato sulla intranet aziendale Normative e Regolamenti - Privacy

I DIRITTI DELL'INTERESSATO.

Art.7 D.Lgs.196/2003 . Si riporta il testo.

“ L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

L'interessato ha diritto di ottenere l'indicazione:a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'art.5, comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

L'interessato ha diritto di ottenere: a)l'aggiornamento, la rettificazione, ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'interessato ha diritto di opporsi in tutto o in parte: a)per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale”.

Istruzioni operative SOCIAL MEDIA

(Linee guida sui social media per i dipendenti)

Premessa

L'Azienda Usl di Imola riconosce che sussistono esigenze professionali per l'utilizzo in azienda dei Social Media. Promuove quindi rapporti di lavoro improntati su collaborazione e fiducia e permette ai propri dipendenti, che ne possono beneficiare professionalmente, di utilizzare i Social Media nel rispetto delle linee guida specificate in questo documento. L'utilizzo dei Social Media è soggetto alle regole riportate nel "Disciplinare Aziendale in merito all'utilizzo degli strumenti elettronici nell'ambito del rapporto di lavoro", reperibile sul sito intranet/internet aziendale. Si richiama in particolare l'art. 1 comma 1 "L'Azienda mette a disposizione dei lavoratori computer, servizi di posta elettronica e internet, esclusivamente per lo svolgimento di compiti istituzionali o comunque correlati alla prestazione lavorativa".

Per ciò che riguarda il rapporto tra l'Ausl di Imola ed i social media, l'ufficio che si occupa della gestione del profilo dell'ente è lo Staff Informazione e Comunicazione ed i contenuti pubblicati si attengono alla mission aziendale.

Cosa sono i Social Media

Per Social Media si intende qualunque sito Web nel quale gli utenti sono in grado di condividere contenuti con molti altri visitatori. I contenuti condivisi possono includere informazioni personali, opinioni, commenti, video, foto, informazioni commerciali, ecc. Esempi di tali applicazioni web, sono: Facebook, Twitter, YouTube e LinkedIn. Anche blog, forum e community sono considerati Social Media.

Autorizzazione all'utilizzo dei Social Media

Compete ai Direttori delle Unità Operative richiedere all'UOTIR l'abilitazione per i propri dipendenti all'utilizzo dei Social Media, tramite gli appositi moduli, scaricabili dalla intranet aziendale. La scelta in merito ai lavoratori da abilitare è effettuata dal Direttore di unità operativa tenendo conto del ruolo e delle mansioni degli operatori stessi, nonché dell'utilità dell'abilitazione ai fini professionali/istituzionali.

Policy per i contenuti inappropriati

I siti e i Social Media con contenuti inappropriati sono di norma bloccati automaticamente dal software di Web Filtering adottato in azienda (Websense); i lavoratori devono comunque utilizzare buon senso e l'ordinaria diligenza nel valutare se i contenuti visualizzati siano appropriati. Qualora

il lavoratore rilevi, incidentalmente, l'accessibilità a siti con contenuti inopportuni, lo segnala all'UOTIR.

Policy sulla pubblicazione di contenuti e sulla riservatezza

I lavoratori sono responsabili dei contenuti che pubblicano nei Social Media, e ne rispondono ai sensi di legge, in sede civile, penale, amministrativa e disciplinare. L'Azienda Usl di Imola, nel caso di pubblicazione di contenuti inappropriati o riservati, si riserva di intervenire.

La circolazione delle informazioni inserite nei social media, non è contenibile, né governabile dall'autore. La pubblicazione di dati sui Social Media, è configurabile come operazione di diffusione del dato ai sensi del Codice Privacy e pertanto soggetta alla speciale disciplina restrittiva prevista dal Dlgs. 196/2003.

Quando si pubblicano contenuti (ad esempio foto, filmati, dati...) oppure si inseriscono post o commenti, si ricorda di:

- a) attenersi alle norme del Codice privacy ed alle istruzioni operative fornite dall'azienda (Istruzioni operative per gli incaricati e per i responsabili del trattamento di dati personali / sensibili / giudiziari),
- b) attenersi alle norme in tema di copyright;
- c) rispettare il Codice di comportamento dei pubblici dipendenti, in particolare non pubblicare contenuti lesivi per l'immagine dell'azienda;
- d) rispettare gli obblighi dei dipendenti indicati nei contratti di lavoro (Codice disciplinare reperibile nel sito Internet dell'Azienda);
- e) non registrare profili utilizzando ragioni sociali o marchi dell'Azienda Usl di Imola o di altre aziende.

A titolo esemplificativo si raccomanda:

- f) -di non divulgare o utilizzare informazioni riservate relative ad altre persone oppure all'Azienda Usl di Imola;
- g) di essere consapevoli che verrete associati all'Azienda Usl di Imola sui Social Media se nel vostro profilo avete specificato di esserne dipendenti. Assicuratevi che il vostro profilo ed i contenuti allegati ad esso, siano coerenti con l'immagine che volete dare di voi;
- h) se avete dubbi sui contenuti che desiderate mettere on-line e gli stessi siano in relazione con l'attività dell'Azienda, parlatene con il vostro responsabile o non pubblicate nulla;

I Social Media sono spesso utilizzati da criminali informatici per diffondere virus, violare sistemi o carpire informazioni riservate. Per ridurre al minimo i rischi, è bene uniformarsi alle linee guida elencate a seguire, considerando sempre che esse non sono esaustive, e che non sostituiscono comunque l'utilizzo del buon senso.

- per i Social Media utilizzati sia in ambito lavorativo che in ambito personale (ad esempio Facebook, Twitter), non utilizzare l'indirizzo mail aziendale in quanto questi Social Media sono piuttosto invasivi e si rischia di ricevere molto spam. E' consigliabile procurarsi una mail da utilizzare solo per i Social Media (*quindi dovremmo dare un altro indirizzo mail ai dipendenti abilitati? Come si gestiscono?*)
- per i Social Media non utilizzare le stesse password che usate per accedere a computer o software aziendali;
- non seguire profili, link, o scaricare software da pagine di Social Media postati da persone o organizzazioni che non si conoscono;
- se il contenuto che si sta visualizzando, su una qualunque pagina web di un Social Media, sembra sospetto, chiudere il browser e non tornare su quella pagina.